

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-130488

(43)Date of publication of application : 19.05.2005

(51)Int.Cl.

H04L 9/32
G06F 12/14

(21)Application number : 2004-290775

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 01.10.2004

(72)Inventor : HOTTA HIDEKAZU
ONO SATOSHI
TAKURA AKIRA

(30)Priority

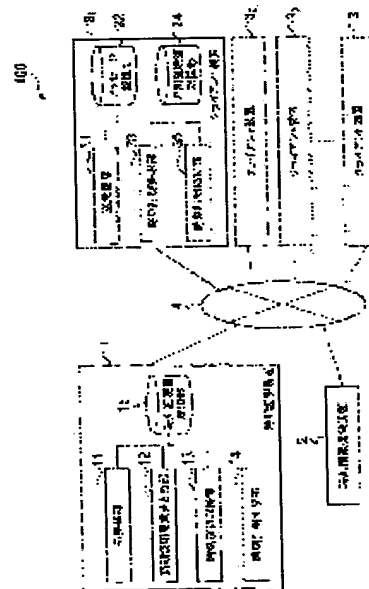
Priority number : 2003345946 Priority date : 03.10.2003 Priority country : JP

(54) TIME CERTIFICATION APPARATUS, TIME CERTIFICATION REQUEST ACCEPTING APPARATUS, TIME CERTIFICATION METHOD, TIME CERTIFICATION REQUEST ACCEPTING METHOD, TIME CERTIFICATION PROGRAM, TIME CERTIFICATION REQUEST ACCEPTANCE PROGRAM, TIME CERTIFICATION VERIFICATION PROGRAM, AND PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To perform time certification with an accurate time, even if there are a number of time certification requests simultaneously from users by utilizing the Merkle hash tree in a time stamp system, based on a public key.

SOLUTION: A time certification apparatus 1 comprises a transmitting/receiving part 11 for exchanging data between a time information providing device 2 and client devices 3i via a computer network 4; a time certification request editing part 12 for editing a message digest transmitted from the client devices 3i as time certification requests, using the Merkle hash tree; a time information acquiring part 13 for acquiring time information from the time information providing device 2, when creating a time certificate; a time certification creating part 14 for creating the time certificate by adding the time information, that is acquired by the time information acquiring part 12, to the message digest edited by the time certification request editing part 12; and a time certificate storage part 15 for storing the time certificate created by the time certification creating part 14.



LEGAL STATUS

[Date of request for examination]

This Page Blank (uspto)

【特許請求の範囲】**【請求項1】**

公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめ、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明装置であって、

前記利用者装置から前記要求を受信する受信手段と、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、

前記所定の時間を決定する時刻情報を提供する時刻情報提供手段と、

前記時刻情報提供手段から提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を前記要求の補完情報として取得する補完情報取得手段と、

前記時刻証明書および前記補完情報を前記利用者装置に送信する送信手段と、を有することを特徴とする時刻証明装置。

【請求項2】

前記時刻証明書作成手段は、

前記まとめが終了したときに前記時刻情報提供手段から提供された現ラウンド終了時刻を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成することを特徴とする請求項1記載の時刻証明装置。

【請求項3】

前記時刻証明要求まとめ手段は、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、

前記時刻証明書作成手段は、

前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供手段から提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、

前記補完情報取得手段は、

前記直前のルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、

前記送信手段は、

前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを特徴とする請求項2記載の時刻証明装置。

【請求項4】

公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求に

時刻情報を付すとともに、二分木を利用してまとめ、まとめた値に対してデジタル署名を生成する時刻証明装置であって、

前記利用者装置から前記要求を受信する受信手段と、

前記要求を受信した時刻情報を提供する時刻情報提供手段と、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供手段から提供される前記時刻情報を接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、

前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、

前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、

前記時刻証明書および前記補完情報を前記利用者装置に送信する送信手段と、を有することを特徴とする時刻証明装置。

【請求項5】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明装置であって、

前記要求に含まれる時刻証明対象データと、前記時刻証明要求受付装置が前記要求を受信した時刻である前記第1の時刻情報との組み合わせである前記第2の要求を前記時刻証明要求受付装置から受信する受信手段と、

前記第2の要求を受信した時刻である第2の時刻情報を提供する時刻情報提供手段と、

前記第1の時刻情報と、前記第2の時刻情報の差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、

前記ルート値から部分署名を生成する部分署名生成手段と、

前記部分署名から全体署名を生成し、該全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書、並びに前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値である補完情報を前記利用者装置に送信する前記時刻証明要求受付装置に、前記部分署名を送信する送信手段と、

を有することを特徴とする時刻証明装置。

【請求項6】

前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを特徴とする請求項1乃至3のいずれか1項に記載の時刻証明装置。

【請求項7】

前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを特徴とする請求項1乃至6のい

れか1項に記載の時刻証明装置。

【請求項8】

前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを特徴とする請求項1乃至6のいずれか1項に記載の時刻証明装置。

【請求項9】

前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを特徴とする請求項1乃至6のいずれか1項に記載の時刻証明装置。

【請求項10】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまとめた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置であって、

前記利用者装置から前記要求を受信する受信手段と、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てる値を計算する時刻証明要求まとめ手段と、

前記二分木のルート値を前記時刻証明装置に送信する送信手段と、

前記二分木のルート値に時刻情報を付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を前記時刻証明装置から受信する時刻証明書受信手段と、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、

前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信手段と、

を有することを特徴とする時刻証明要求受付装置。

【請求項11】

前記時刻証明書受信手段は、

前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信することを特徴とする請求項10記載の時刻証明要求受付装置。

【請求項12】

前記時刻証明要求まとめ手段は、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、

前記送信手段は、

前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直前ルート値及び前記前ラウンド終了時刻を前記前記時刻証明装置に送信し、

前記時刻証明書受信手段は、

前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、

前記補完情報取得手段は、

前記直前ルート値を割当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、

前記時刻証明書送信手段は、

前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを特徴とする請求項 1 記載の時刻証明要求受付装置。

【請求項13】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第 1 の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第 1 の時刻情報を付与した第 2 の要求を受け付けて、所定の時間内における、複数の前記第 2 の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置であって、

前記利用者装置から前記要求を受信する受信手段と、

前記要求に含まれる時刻証明対象データと、前記要求を受信した時刻である前記第 1 の時刻情報と、の組み合わせである前記第 2 の要求を前記複数の時刻証明装置それぞれに送信する送信手段と、

前記複数の時刻証明装置それぞれが、前記第 1 の時刻情報と前記第 2 の要求を受信した時刻である第 2 の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第 2 の要求に含まれる前記要求内の時刻証明対象データと前記第 1 の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信手段と、

前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第 1 の時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、

前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、

前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信手段と、を有することを特徴とする時刻証明要求受付装置。

【請求項14】

前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを特徴とする請求項 1 0 乃至 1 2 のいずれか 1 項に記載の時刻証明要求受付装置。

【請求項15】

前記部分署名は、閾値型の分散署名方式であり、前記時刻証明書作成手段は、前記複数の時刻証明装置から受信した部分署名が所定の数以上ある場合には、全体署名を生成することを特徴とする請求項 1 3 記載の時刻証明要求受付装置。

【請求項16】

前記二分木は、前記要求の数が確定した後に、深さの違いを 1 以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを特徴とする請求項 1 0 乃至 1 5 のいずれか 1 項に記載の時刻証明要求受付装置。

【請求項17】

前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを特徴とする請求項10乃至15のいずれか1項に記載の時刻証明要求受付装置。

【請求項18】

前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを特徴とする請求項10乃至15のいずれか1項に記載の時刻証明要求受付装置。

【請求項19】

公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求を二分木を利用してまとめ、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明方法であって、

前記利用者装置から前記要求を受信する受信ステップと、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求の値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、

前記所定の時間を決定する時刻情報を提供する時刻情報提供ステップと、

前記時刻情報提供ステップにおいて提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を前記要求の補完情報として取得する補完情報取得ステップと、

前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、を有することを特徴とする時刻証明方法。

【請求項20】

前記時刻証明書作成ステップは、

前記まとめが終了したときに前記時刻情報提供ステップから提供された現ラウンド終了時刻を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成することを特徴とする請求項19記載の時刻証明方法。

【請求項21】

前記時刻証明要求まとめステップは、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、

前記時刻証明書作成ステップは、

前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供ステップから提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、

前記補完情報取得ステップは、

さらに、前記直前のルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取

得し、

前記送信ステップは、

さらに、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを特徴とする請求項20記載の時刻証明方法。

【請求項22】

公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求に時刻情報を付すとともに、二分木を利用してまとめ、まとめた値に対してデジタル署名を生成する時刻証明方法であって、

前記利用者装置から前記要求を受信する受信ステップと、

前記要求を受信した時刻情報を提供する時刻情報提供ステップと、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供ステップで提供される前記時刻情報を接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、

前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、

前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、

前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、を有することを特徴とする時刻証明方法。

【請求項23】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明装置の時刻証明方法であって、

前記要求に含まれる時刻証明対象データと、前記時刻証明要求受付装置が前記要求を受信した時刻である前記第1の時刻情報との組み合わせである前記第2の要求を前記時刻証明要求受付装置から受信する受信ステップと、

前記第2の要求を受信した時刻である第2の時刻情報を提供する時刻情報提供ステップと、

前記第1の時刻情報と、前記第2の時刻情報の差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、

前記ルート値から部分署名を生成する部分署名生成ステップと、

前記部分署名から全体署名を生成し、該全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書、並びに前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値である補完情報を前記利用者装置に送信する前記時刻証明要求受付装置に、前記部分署名を送信する送信ステップと、

を有することを特徴とする時刻証明方法。

【請求項24】

前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを特徴とする請求項19乃至21のいずれか1項に記載の時刻証明方法。

【請求項25】

前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを特徴とする請求項19乃至24のいずれか1項に記載の時刻証明方法。

【請求項26】

前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを特徴とする請求項19乃至24のいずれか1項に記載の時刻証明方法。

【請求項27】

前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを特徴とする請求項19乃至24のいずれか1項に記載の時刻証明方法。

【請求項28】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまとめた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付方法であって、

前記利用者装置から前記要求を受信する受信ステップと、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てる値を計算する時刻証明要求まとめステップと、

前記二分木のルート値を前記時刻証明装置に送信する送信ステップと、

前記二分木のルート値に時刻情報を付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を前記時刻証明装置から受信する時刻証明書受信ステップと、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、

前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、

を有することを特徴とする時刻証明要求受付方法。

【請求項29】

前記時刻証明書受信ステップは、

前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信することを特徴とする請求項28記載の時刻証明要求受付方法。

【請求項30】

前記時刻証明要求まとめステップは、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定

の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割当て、

前記送信ステップは、

前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直前ルート値及び前記前ラウンド終了時刻を前記前記時刻証明装置に送信し、

前記時刻証明書受信ステップは、

前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、

前記補完情報取得ステップは、

前記直前ルート値を割当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、

前記時刻証明書送信ステップは、

前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを特徴とする請求項 2 9 記載の時刻証明要求受付方法。

【請求項31】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第 1 の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第 1 の時刻情報を付与した第 2 の要求を受け付けて、所定の時間内における、複数の前記第 2 の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付方法であって、

前記利用者装置から前記要求を受信する受信ステップと、

前記要求に含まれる時刻証明対象データと、前記要求を受信した時刻である前記第 1 の時刻情報と、の組み合わせである前記第 2 の要求を前記複数の時刻証明装置それぞれに送信する送信ステップと、

前記複数の時刻証明装置それぞれが、前記第 1 の時刻情報と前記第 2 の要求を受信した時刻である第 2 の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第 2 の要求に含まれる前記要求内の時刻証明対象データと前記第 1 の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信ステップと、

前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第 1 の時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、

前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、

前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、

を有することを特徴とする時刻証明要求受付方法。

【請求項32】

前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを特徴とする請求項 2 8 乃至 3 0 のいずれか 1 項に記載の時刻証明要求受付方法。

【請求項33】

前記部分署名は、閾値型の分散署名方式であり、前記時刻証明書作成ステップは、前記複数の時刻証明装置から受信した部分署名が所定の数以上ある場合には、全体署名を生成することを特徴とする請求項31記載の時刻証明要求受付方法。

【請求項34】

前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを特徴とする請求項28乃至33のいずれか1項に記載の時刻証明要求受付方法。

【請求項35】

前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを特徴とする請求項28乃至33のいずれか1項に記載の時刻証明要求受付方法。

【請求項36】

前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを特徴とする請求項28乃至33のいずれか1項に記載の時刻証明要求受付方法。

【請求項37】

公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求を二分木を利用してまとめ、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明プログラムであって、

前記利用者装置から前記要求を受信する受信ステップと、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求の値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、

前記所定の時間を決定する時刻情報を提供する時刻情報提供ステップと、

前記時刻情報提供ステップにおいて提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を前記要求の補完情報として取得する補完情報取得ステップと、

前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、
を前記時刻証明装置に実行させることを特徴とする時刻証明プログラム。

【請求項38】

前記時刻証明書作成ステップは、

前記まとめが終了したときに前記時刻情報提供ステップから提供された現ラウンド終了時刻を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成することを特徴とする請求項37記載の時刻証明プログラム。

【請求項39】

前記時刻証明要求まとめステップは、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、

前記時刻証明書作成ステップは、

前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供ステップから提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、

前記補完情報取得ステップは、

さらに、前記直前のルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、

前記送信ステップは、

さらに、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを特徴とする請求項38記載の時刻証明プログラム。

【請求項40】

公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求に時刻情報を付すとともに、二分木を利用してまとめ、まとめた値に対してデジタル署名を生成する時刻証明プログラムであって、

前記利用者装置から前記要求を受信する受信ステップと、

前記要求を受信した時刻情報を提供する時刻情報提供ステップと、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供ステップで提供される前記時刻情報を接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、

前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、

前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、

前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、を前記時刻証明装置に実行させることを特徴とする時刻証明プログラム。

【請求項41】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明装置の時刻証明プログラムであって、

前記要求に含まれる時刻証明対象データと、時刻証明要求受付装置が前記要求を受信した時刻である前記第1の時刻情報との組み合わせである前記第2の要求を前記時刻証明要求受付装置から受信する受信ステップと、

前記第2の要求を受信した時刻である第2の時刻情報を提供する時刻情報提供ステップと、

前記第1の時刻情報と、前記第2の時刻情報の差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイ

ジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、

前記ルート値から部分署名を生成する部分署名生成ステップと、

前記部分署名から全体署名を生成し、該全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書、並びに前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値である補完情報を前記利用者装置に送信する前記時刻証明要求受付装置に、前記部分署名を送信する送信ステップと、

を前記時刻証明装置に実行させることを特徴とする時刻証明プログラム。

【請求項42】

前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを特徴とする請求項37乃至39のいずれか1項に記載の時刻証明プログラム。

【請求項43】

前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを特徴とする請求項37乃至42のいずれか1項に記載の時刻証明プログラム。

【請求項44】

前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを特徴とする請求項37乃至42のいずれか1項に記載の時刻証明プログラム。

【請求項45】

前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを特徴とする請求項37乃至42のいずれか1項に記載の時刻証明プログラム。

【請求項46】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまとめた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付プログラムであって、

前記利用者装置から前記要求を受信する受信ステップと、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てる値を計算する時刻証明要求まとめステップと、

前記二分木のルート値を前記時刻証明装置に送信する送信ステップと、

前記二分木のルート値に時刻情報を付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を前記時刻証明装置から受信する時刻証明書受信ステップと、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、

前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、

を前記時刻証明要求受付装置に実行させることを特徴とする時刻証明要求受付プログラム。

。

【請求項47】

前記時刻証明書受信ステップは、

前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信することを特徴とする請求項46記載の時刻証明要求受付プログラム。

【請求項48】

前記時刻証明要求まとめステップは、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、

前記送信ステップは、

前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直前ルート値及び前記前ラウンド終了時刻を前記前記時刻証明装置に送信し、

前記時刻証明書受信ステップは、

前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、

前記補完情報取得ステップは、

前記直前ルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、

前記時刻証明書送信ステップは、

前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを特徴とする請求項47記載の時刻証明要求受付プログラム。

【請求項49】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付プログラムであって、

前記利用者装置から前記要求を受信する受信ステップと、

前記要求に含まれる時刻証明対象データと、前記要求を受信した時刻である前記第1の時刻情報と、の組み合わせである前記第2の要求を前記複数の時刻証明装置それぞれに送信する送信ステップと、

前記複数の時刻証明装置それぞれが、前記第1の時刻情報と前記第2の要求を受信した時刻である第2の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信ステップと、

前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト

、および前記第1の時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、
前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、
前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、
を前記時刻証明要求受付装置に実行させることを特徴とする時刻証明要求受付プログラム。

【請求項50】

前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを特徴とする請求項46及び48のいずれか1項に記載の時刻証明要求受付プログラム。

【請求項51】

前記部分署名は、閾値型の分散署名方式であり、前記時刻証明書作成ステップは、前記複数の時刻証明装置から受信した部分署名が所定の数以上ある場合には、全体署名を生成することを特徴とする請求項49記載の時刻証明要求受付プログラム。

【請求項52】

前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを特徴とする請求項46乃至51のいずれか1項に記載の時刻証明要求受付プログラム。

【請求項53】

前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを特徴とする請求項46乃至51のいずれか1項に記載の時刻証明要求受付プログラム。

【請求項54】

前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを特徴とする請求項46乃至51のいずれか1項に記載の時刻証明要求受付プログラム。

【請求項55】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめて、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、

前記所定の時間を決定する時刻情報を提供する時刻情報提供手段と、

前記時刻情報提供手段から提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された時刻情報を含む前記時刻証明書を作成する時刻証明書作成手段と、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する前記時刻証明装置から

前記時刻証明書および前記補完情報を受信する受信ステップと、

前記時刻証明装置に送信した前記要求および前記補完情報から計算した前記二分木のルート値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第1の検証ステップと、

前記時刻証明書に含まれる前記デジタル署名が前記ルート値および前記時刻情報を接続

した接続値に対して為されたものであるか否かを検証する第2の検証ステップと、
を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項56】

前記時刻証明書作成手段は、

前記まとめが終了したときに前記時刻情報提供手段から提供された現ラウンド終了時刻
を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付さ
れた前記現ラウンド終了時刻を含み、前記要求の受付け時刻が、前記現ラウンド終了時刻
より前であることを証明する時刻証明書を作成し、

前記第2の検証ステップは、

前記時刻証明書に含まれる前記デジタル署名が前記ルート値および現ラウンド終了時刻
を接続した接続値に対して為されたものであるか否かを検証することを特徴とする請求項
55記載の時刻証明検証プログラム。

【請求項57】

前記時刻証明要求まとめ手段は、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定
の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルー
ト値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリー
フに前記直前ルート値を割当て、

前記時刻証明書作成手段は、

前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供ステ
ップから提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終
了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、
前記要求の受付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻
より前であることを証明する時刻証明書を作成し、

前記補完情報取得手段は、

前記直前のルート値を割当てられた前記二分木のリーフから該二分木のルート値を計算
するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、

前記送信手段は、

前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信し、

前記直前ルート値および前記直前ルート値の補完情報から計算した前記二分木のルート
値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第3の検
証ステップと、
を前記利用者装置に実行させることを特徴とする請求項56記載の時刻証明検証プログラ
ム。

【請求項58】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコン
ピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を
二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまと
めた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報
を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムス
タンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、

前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリー
フに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続
した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに
割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当
てるルート値を計算する時刻証明要求まとめ手段と、

前記所定の時間を決定する時刻情報を前記ルート値に付して施したデジタル署名、前記
ルート値、および前記ルート値に付された時刻情報を含む前記時刻証明書を前記時刻証明
装置から受信する時刻証明書受信手段と、

前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木の

ルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する前記時刻証明要求受付装置から

前記時刻証明書および前記補完情報を受信する受信ステップと、

前記時刻証明要求受付装置に送信した前記要求および前記補完情報から計算した前記二分木のルート値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第1の検証ステップと、

前記時刻証明書に含まれる前記デジタル署名が前記ルート値および前記時刻情報を接続した接続値に対して為されたものであるか否かを検証する第2の検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項59】

前記時刻証明書受信手段は、

前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、

前記第2の検証ステップは、

前記時刻証明書に含まれる前記デジタル署名が前記ルート値および前記現ラウンド終了時刻を接続した接続値に対して為されたものであるか否かを検証することを特徴とする請求項58記載の時刻証明検証プログラム。

【請求項60】

前記時刻証明要求まとめ手段は、

前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割当て、

前記時刻証明要求受付装置は、

前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直前ルート値及び前記前ラウンド終了時刻を前記前記時刻証明装置に送信する手段を有し、

前記時刻証明書受信手段は、

前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し

前記補完情報取得手段は、

前記直前ルート値を割当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、

前記受信ステップは、

前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置から受信し、

前記直前ルート値および前記直前ルート値の補完情報から計算した前記二分木のルート値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第3の検証ステップと、

を前記利用者装置に実行させることを特徴とする請求項59記載の時刻証明検証プログラム。

【請求項61】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求に時刻情報を付すとともに、二分木を利用してまとめて、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、

前記要求を受信した時刻情報を提供する時刻情報提供手段と、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供手段から提供される前記時刻情報を接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記ダイジェストの値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む前記時刻証明書を作成する時刻証明書作成手段と、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する時刻証明装置から前記時刻証明書および前記補完情報を受信する受信ステップと、

前記時刻証明装置に送信した前記要求に含まれる時刻証明対象データと前記時刻証明書に含まれる前記時刻情報とを接続した接続値のダイジェストと、前記時刻証明書に含まれる前記リーフに割り当てられた前記ダイジェストと、が一致するか否かを検証する第1の検証ステップと、

前記時刻証明書に含まれるデジタル署名が前記時刻証明書に含まれる、前記リーフに割り当てられた前記ダイジェストおよび前記補完情報から計算された前記二分木のルート値に対して為されたものであるか否かを検証する第2の検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項62】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、

前記要求に含まれる時刻証明対象データと、前記時刻証明要求受付装置が前記要求を受信した時刻情報である前記第1の時刻情報と、の組み合わせである前記第2の要求を前記複数の時刻証明装置それぞれに送信する送信手段と、前記複数の時刻証明装置それぞれが、前記第1の時刻情報と前記第2の要求を受信した時刻である第2の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信手段と、前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト、前記第1の時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する前記時刻証明要求受付装置から前記時刻証明書および前記補完情報を受信する受信ステップと、

前記時刻証明要求受付装置に送信した前記要求に含まれる時刻証明対象データと前記時刻証明書に含まれる前記時刻情報とを接続した接続値のダイジェストと、前記時刻証明書に含まれる前記リーフに割り当てられた前記ダイジェストと、が一致するか否かを検証する第1の検証ステップと、

前記時刻証明書に含まれる前記全体署名が前記時刻証明書に含まれる、前記リーフに割り当てられた前記ダイジェストおよび前記補完情報から計算された前記二分木のルート値に対して為されたか否かを検証する第2の検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項63】

請求項37乃至62のいずれか1項に記載されたプログラムを記録したことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、PKI (Public Key Infrastructure ; 公開鍵基盤) におけるタイムスタンプ技術に関し、より詳しくは、2分木 (Merkle tree) を利用して時刻証明を行う時刻証明装置、時刻証明要求受付装置、時刻証明方法、時刻証明要求受付方法、時刻証明プログラム、時刻証明要求受付プログラム、時刻証明検証プログラム、およびプログラム記録媒体に関する。

【背景技術】

【0002】

タイムスタンプ技術は、デジタルデータがある特定時刻に存在していたことを証明するとともに、その時刻以降データが変更されていないことを証明する技術である。近年、インターネット上での電子商取引の活発化や、デジタル文書管理の利用拡大に伴い、「誰が、いつ、どんなデータを生成し、送信したか」を第三者が証明する電子公証の仕組みが必要とされている。電子公証は、送受信者の特定、到達確認、時刻情報の付与、改ざんの検知、電子文書保管等の機能を具備するものであるが、タイムスタンプ技術は、このうち、時刻情報の付与及び改ざんの検知の機能を実現するものである。

【0003】

図17は、このようなタイムスタンプ技術を用いたタイムスタンプシステムである。同図に示すタイムスタンプシステム900は、利用者(要求者、検証者)30がタイムスタンプの対象データをTSA (Time Stamping Authority ; タイムスタンプ生成機関) 10に送信すると、TSA 10がTA (Time Authority ; 時刻源である時刻情報提供機関) 20から時刻情報を入手して、利用者30から要求された対象データに対してタイムスタンプを生成し、該タイムスタンプを利用者30に返信するようになっている。そして、このTSA 10で発行されるタイムスタンプは、通常、利用者30から送られる対象データに時刻情報を付した結果である署名対象データに対して生成したデジタル署名を含む時刻証明書となっている。

【0004】

尚、この出願に関連する先行技術文献情報としては、次のものがある。

【0005】

ここで、非特許文献1では、図17のTSA 10において公開鍵基盤とデジタル署名を用いることによりタイムスタンプを生成する方式について述べている。

【0006】

非特許文献2では、前もって定められた一定時間(例えば1秒間、これをラウンドという)に受け付けた時刻証明要求を2分木等を用いて、集約ハッシュ値と呼ばれる1つのハッシュ値に集約して該集約ハッシュ値含む時刻証明書を発行し、また該時刻証明書を該集約間隔より前に同様に生成された時刻証明書を結合してそれら時刻証明書の生成順序を偽造不可能な形で証明するようなリンク情報を生成し、さらに前もって定められた公開間隔(例えば1週間)毎に該リンク情報を公表することにより、デジタルデータがある特定時刻に存在していたことを証明するとともに、その時刻以降データが変更されていないことを証明することを可能とするタイムスタンプ方式を記述している。尚、この方式においては公開鍵基盤とデジタル署名はタイムスタンプを実現するための主要な手段ではなく、用いられないかまたは補助的に用いられるのみである。

【非特許文献1】ISO/IEC IS 18014-2 Information technology--Security techniques--Time-stamping services--Part 2: Mechanisms producing independent tokens

【非特許文献2】ISO/IEC IS 18014-3 Information technology--Security techniques--

Time-stamping services--Part 3: Mechanisms producing linked tokens

【非特許文献3】D. Pinkas et al.: Electronic signature formats for long term electronic signatures (RFC 3126), 2001, IETF.

【発明の開示】

【発明が解決しようとする課題】

【0007】

タイムスタンプ・システムに対する要件として、以下の5つの条件が挙げられる。第1には、予想される時刻証明要求を処理するために十分な、タイムスタンプの生成のための処理能力を持つことである。第2には、公開鍵基盤とデジタル署名を用いる方式を採用する場合には、デジタル署名の有効性の根拠となる公開鍵証明書に有効期限があるため時刻証明書の有効期限延長のための処理が必要となるが、この有効期限延長を容易に実現する手順が存在しかつこの手順を実行するために十分な処理能力を持つことである。第3には、時刻証明要求を TSA に送信し時刻証明書を受信するクライアントは、時刻証明書の正当性を検証できることであるが、この際、時刻証明書の受信時に、遅滞なく即時に当該の時刻証明書の正当性を検証できることが望ましく、また発行された時刻証明書に付された時刻とその元となった時刻証明要求のTSAによる受付けの時刻が如何なる関係であるかが明確であることが望ましい。第4には、TSA におけるプログラムによる処理においては、プログラム上のエラーが逸早く検出可能で、エラーの影響が限定されるという意味でプログラム上のエラーに対して高い耐性を持つことである。第5には、TSAのサービスが災害やビジネス上の理由で継続不能となったとき、時刻証明書の正当性を保証する方法が存在することであるが、この際この保証方法を実行する上で、タイムスタンプ・サービスのクライアントに対する負荷が小さいことが望ましい。

【0008】

非特許文献1で述べられている、TSAにおいて公開鍵基盤とデジタル署名を用いることによりタイムスタンプを生成する方式は、前述のタイムスタンプ・システムに対する要件に照らして、次のような問題点がある。まず上記第1の要件に関して、公開鍵基盤を前提としたタイムスタンプシステム900においてデジタル署名の処理量が大きいため、利用者30からタイムスタンプの要求が多く、一時的に集中するような場合には、TSA10に設けられた時刻証明装置は、正確な時刻情報を付して時刻証明を行うことが困難であるという問題がある。また、上記第2の要件に関しては、該方式は公開鍵基盤とデジタル署名を用いることによりタイムスタンプを生成する方式であるため、非特許文献3で述べられているように公開鍵の有効期限が切れる前にタイムスタンプの延長処理を行う必要があるが、この際の処理量が大きいため、及びこの延長処理を行うためにタイムスタンプ受領者による手続きが必要となるという問題がある。

【0009】

尚、上記の要件のうち第3、第4、第5については、該方式に大きな問題はない。まず上記第3の要件に関して、該方式は、デジタル署名の検証機能と公開鍵基盤の提供する公開鍵証明書の有効性検証機能により、受理した時刻証明書の有効性を即時に検証できるため問題はない。上記第4の要件に関して、該方式は、時刻証明書を発行する上でのプログラム上のエラーは、個々の時刻証明書の検証を行うことにより発見可能であり、ある時刻証明書を発行する上でのプログラム上のエラーはその時刻証明書のみに影響するという意味で、プログラム上のエラーに対して高い耐性を持ち問題はない。上記第5の要件に関して、該方式は、TSAのサービスが災害やビジネス上の理由で継続不能になっても、時刻証明書作成に用いられた署名鍵に対応する公開鍵証明書の、時刻証明を行った時点における有効性が CA (Certificate Authority) 等により保証される限りは、非特許文献3で記載された再署名の方法等により時刻証明書の有効性を保持することが出来るため問題はない。

【0010】

非特許文献2で述べられている、時刻証明要求の集約、リンク情報の生成、及びリンク情報の定期的な公表を利用する方式は、前述のタイムスタンプ・システムに対する要件に

照らして、次のような問題点がある。上記第3の要件に関して、該方式においては、時刻証明要求を送付したクライアントは、受領した時刻証明書の正しさを、上記の公開間隔が終わるまで検証することが出来ないという意味で即時検証性がないという問題がある。また発行された時刻証明書に付された時刻は、所定の方法で集約される複数の時刻証明要求に対して同一の値とすることになっており、この時刻と、該複数の時刻証明要求に属する個々の時刻証明要求のTSAによる受付けの時刻が如何なる関係であるかが明確でないという問題点がある。上記第4の要件に関して、該方式においては、以下の意味でプログラム・ロジックに対する耐性が小さいという問題がある。即ち、ある時刻証明書をそれより前に発行された時刻証明書と結合するリンク情報を生成する処理のプログラム・ロジックが比較的複雑でエラーが混入する可能性があるが、もしエラーがあった場合には、上記の公開間隔が終わるまで検出することが困難で、かつエラーが検出されたときには当該の公開間隔に発行された全ての時刻証明書に影響を及ぼす可能性がある。上記第5の要件に関して、該方式においては、TSAのサービスが災害やビジネス上の理由で継続不能となったとき、あるクライアントがあるラウンドで受理した時刻証明書がある公表間隔で発行されたこと等、該時刻証明書の正当性を保証するためには、公表間隔（例えば1週間）の間に各ラウンドで発行した全ての時刻証明書の集約ハッシュ値を該クライアントは取得し保存する必要がある。この集約ハッシュ値の個数は、例えばラウンドが1秒で公表間隔が1週間のとき604800個となり、時刻証明書の正当性を保証するためにクライアントが取得・保存しなければならぬデータの量が膨大になるという問題がある。

【0011】

尚、上記の要件のうち第1、第2については、該方式に大きな問題はない。まず上記第1の要件に関して、該方式は、時刻証明書の発行に際して、処理量の多いデジタル署名ではなく、高速実行できるハッシュ関数を用いているため問題はない。また、上記第2の要件に関して、該方式は公開鍵基盤やデジタル署名を用いていないため、公開鍵証明書の有効期限による時刻証明書の延長処理を行う必要がないため問題はない。

【0012】

本発明は、上記の課題を解決するためになされたものであり、公開鍵基盤に基づくタイムスタンプシステムにおいて二分木を利用することにより、前記5つの要件を満たすような時刻証明装置、時刻証明要求受付装置、時刻証明方法、時刻証明要求受付方法、時刻証明プログラム、時刻証明要求受付プログラム、時刻証明検証プログラム、およびプログラム記録媒体を提供することを目的とする。即ち、第1に、利用者から一時的に多くの時刻証明要求があっても、正確な時刻を付して時刻証明を行うことができ、第2に、時刻証明書の有効期限延長を容易に実現する手順が存在しかつこの手順を実行するために十分な処理能力を持ち、第3に、タイムスタンプ・サービスのクライアントは時刻証明書を受理したときに遅滞なく即時に当該の時刻証明書の正当性を検証でき、第4に、TSAにおけるプログラムによる処理においては、プログラム上のエラーが逸早く検出可能でエラーの影響が限定されるという意味でプログラム上のエラーに対して高い耐性を持ち、第5に、TSAのサービスが災害やビジネス上の理由で継続不能となったとき、時刻証明書の正当性を保証する方法があり、この保証方法を実行する上で、TSAのサービスのクライアントに対する負荷が小さいような時刻証明装置、時刻証明要求受付装置、時刻証明方法、時刻証明要求受付方法、時刻証明プログラム、時刻証明要求受付プログラム、時刻証明検証プログラム、およびプログラム記録媒体を提供することを目的とする。

【課題を解決するための手段】

【0013】

上記目的を達成するため、請求項1記載の本発明は、公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめ、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明装置であって、前記利用者装置から前記要求を受信する受信手段と、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの

子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、前記所定の時間を決定する時刻情報を提供する時刻情報提供手段と、前記時刻情報提供手段から提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を前記要求の補完情報として取得する補完情報取得手段と、前記時刻証明書および前記補完情報を前記利用者装置に送信する送信手段と、を有することを要旨とする。

【0014】

請求項2記載の本発明は、請求項1記載の発明において、前記時刻証明書作成手段は、前記まとめが終了したときに前記時刻情報提供手段から提供された現ラウンド終了時刻を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成することを要旨とする。

【0015】

請求項3記載の本発明は、請求項2記載の発明において、前記時刻証明要求まとめ手段は、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、前記時刻証明書作成手段は、前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供手段から提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受付け時刻が、前記前ラウンド終了時刻より後かつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、前記補完情報取得手段は、前記直前のルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記送信手段は、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを要旨とする。

【0016】

請求項4記載の本発明は、公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求に時刻情報を付すとともに、二分木を利用してまとめ、まとめた値に対してデジタル署名を生成する時刻証明装置であって、前記利用者装置から前記要求を受信する受信手段と、前記要求を受信した時刻情報を提供する時刻情報提供手段と、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供手段から提供される前記時刻情報を接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、前記時刻証明書および前記補完情報を前記利用者装置に送信する送信手段と、を有することを要旨とする。

【0017】

請求項5記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含

まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明装置であって、前記要求に含まれる時刻証明対象データと、前記時刻証明要求受付装置が前記要求を受信した時刻である前記第1の時刻情報との組み合わせである前記第2の要求を前記時刻証明要求受付装置から受信する受信手段と、前記第2の要求を受信した時刻である第2の時刻情報を提供する時刻情報提供手段と、前記第1の時刻情報と、前記第2の時刻情報の差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、前記ルート値から部分署名を生成する部分署名生成手段と、前記部分署名から全体署名を生成し、該全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書、並びに前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値である補完情報を前記利用者装置に送信する前記時刻証明要求受付装置に、前記部分署名を送信する送信手段と、を有することを要旨とする。

【0018】

請求項6記載の本発明は、請求項1乃至3のいずれか1項に記載の発明において、前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを要旨とする。

【0019】

請求項7記載の本発明は、請求項1乃至6のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを要旨とする。

【0020】

請求項8記載の本発明は、請求項1乃至6のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを要旨とする。

【0021】

請求項9記載の本発明は、請求項1乃至6のいずれか1項に記載の発明において、前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを要旨とする。

【0022】

請求項10記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまとめた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置であって、前記利用者装置から前記要求を受信する受信手段と、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てる値を計算する時刻証明要求まとめ手段と、前記二分木のルート値を前記時刻証明装置に送信する送信手段と、前記二分木の

ルート値に時刻情報を付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を前記時刻証明装置から受信する時刻証明書受信手段と、前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信手段と、を有することを要旨とする。

【0023】

請求項 1 1 記載の本発明は、請求項 1 0 記載の発明において、前記時刻証明書受信手段は、前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信することを要旨とする。

【0024】

請求項 1 2 記載の本発明は、請求項 1 1 記載の発明において、前記時刻証明要求まとめ手段は、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、前記送信手段は、前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直前ルート値及び前記前ラウンド終了時刻を前記前記時刻証明装置に送信し、前記時刻証明書受信手段は、前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、前記補完情報取得手段は、前記直前ルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記時刻証明書送信手段は、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを要旨とする。

【0025】

請求項 1 3 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第 1 の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第 1 の時刻情報を付与した第 2 の要求を受け付けて、所定の時間内における、複数の前記第 2 の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置であって、前記利用者装置から前記要求を受信する受信手段と、前記要求に含まれる時刻証明対象データと、前記要求を受信した時刻である前記第 1 の時刻情報と、の組み合わせである前記第 2 の要求を前記複数の時刻証明装置それぞれに送信する送信手段と、前記複数の時刻証明装置それぞれが、前記第 1 の時刻情報と前記第 2 の要求を受信した時刻である第 2 の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第 2 の要求に含まれる前記要求内の時刻証明対象データと前記第 1 の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信手段と、前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第 1 の時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノード

の値を補完情報として取得する補完情報取得手段と、前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信手段と、を有することを要旨とする。

【0026】

請求項14記載の本発明は請求項10乃至12のいずれか1項に記載の発明において、前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを要旨とする。

【0027】

請求項15記載の本発明は、請求項9記載の発明において、前記部分署名は、閾値型の分散署名方式であり、前記時刻証明書作成手段は、前記複数の時刻証明装置から受信した部分署名が所定の数以上ある場合には、全体署名を生成することを要旨とする。

【0028】

請求項16記載の本発明は、請求項10乃至15のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを要旨とする。

【0029】

請求項17記載の本発明は、請求項10乃至15のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを要旨とする。

【0030】

請求項18記載の本発明は、請求項10乃至15のいずれか1項に記載の発明において、前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを要旨とする。

【0031】

請求項19記載の本発明は、公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求を二分木を利用してまとめ、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明方法であって、前記利用者装置から前記要求を受信する受信ステップと、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求の値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、前記所定の時間を決定する時刻情報を提供する時刻情報提供ステップと、前記時刻情報提供ステップにおいて提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を前記要求の補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、を有することを要旨とする。

【0032】

請求項20記載の本発明は、請求項19記載の発明において、前記時刻証明書作成ステップは、前記まとめが終了したときに前記時刻情報提供ステップから提供された現ラウンド終了時刻を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成することを要旨とする。

【0033】

請求項21記載の本発明は、請求項20記載の発明において、前記時刻証明要求まとめステップは、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の

所定のリーフに前記直前ルート値を割当て、前記時刻証明書作成ステップは、前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供ステップから提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、前記補完情報取得ステップは、前記直前のルート値を割当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記送信ステップは、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを要旨とする。

【0034】

請求項2記載の本発明は、公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求に時刻情報を付すとともに、二分木を利用してまとめ、まとめた値に対してデジタル署名を生成する時刻証明方法であって、前記利用者装置から前記要求を受信する受信ステップと、前記要求を受信した時刻情報を提供する時刻情報提供ステップと、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供ステップで提供される前記時刻情報を接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、を有することを要旨とする。

【0035】

請求項2記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明装置の時刻証明方法であって、前記要求に含まれる時刻証明対象データと、前記時刻証明要求受付装置が前記要求を受信した時刻である前記第1の時刻情報との組み合わせである前記第2の要求を前記時刻証明要求受付装置から受信する受信ステップと、前記第2の要求を受信した時刻である第2の時刻情報を提供する時刻情報提供ステップと、前記第1の時刻情報と、前記第2の時刻情報の差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、前記ルート値から部分署名を生成する部分署名生成ステップと、前記部分署名から全体署名を生成し、該全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書、並びに前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値である補完情報を前記利用者装置に送信する前記時刻証明要求受付装置に、前記部分署名を送信する送信

ステップと、を有することを要旨とする。

【0036】

請求項24記載の本発明は、請求項19乃至21のいずれか1項に記載の発明において、前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを要旨とする。

【0037】

請求項25記載の本発明は、請求項19乃至24のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを要旨とする。

【0038】

請求項26記載の本発明は、請求項19乃至24のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを要旨とする。

【0039】

請求項27記載の本発明は、請求項19乃至24のいずれか1項に記載の発明において、前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを要旨とする。

【0040】

請求項28記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまとめた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付方法であって、前記利用者装置から前記要求を受信する受信ステップと、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てる値を計算する時刻証明要求まとめステップと、前記二分木のルート値を前記時刻証明装置に送信する送信ステップと、前記二分木のルート値に時刻情報を付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を前記時刻証明装置から受信する時刻証明書受信ステップと、前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、を有することを要旨とする。

【0041】

請求項29記載の本発明は、請求項28記載の発明において、前記時刻証明書受信ステップは、前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信することを要旨とする。

【0042】

請求項30記載の本発明は、請求項29記載の発明において、前記時刻証明要求まとめステップは、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、前記送信ステップは、前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直

前ルート値及び前記前ラウンド終了時刻を前記前時刻証明装置に送信し、前記時刻証明書受信ステップは、前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、前記補完情報取得ステップは、前記直前ルート値を割当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記時刻証明書送信ステップは、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを要旨とする。

【0043】

請求項3 1記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付方法であって、前記利用者装置から前記要求を受信する受信ステップと、前記要求に含まれる時刻証明対象データと、前記要求を受信した時刻である前記第1の時刻情報と、の組み合わせである前記第2の要求を前記複数の時刻証明装置それぞれに送信する送信ステップと、前記複数の時刻証明装置それぞれが、前記第1の時刻情報と前記第2の要求を受信した時刻である第2の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信ステップと、前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、を有することを要旨とする。

【0044】

請求項3 2記載の本発明は、請求項2 8乃至3 0のいずれか1項に記載の発明において、前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを要旨とする。

【0045】

請求項3 3記載の本発明は、請求項3 1記載の発明において、前記部分署名は、閾値型の分散署名方式であり、前記時刻証明書作成ステップは、前記複数の時刻証明装置から受信した部分署名が所定の数以上ある場合には、全体署名を生成することを要旨とする。

【0046】

請求項3 4記載の本発明は請求項2 8乃至3 3のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを要旨とする。

【0047】

請求項3 5記載の本発明は、請求項2 8乃至3 3のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを要旨とする。

【0048】

請求項36記載の本発明は、請求項28乃至33のいずれか1項に記載の発明において、前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを要旨とする。

【0049】

請求項37記載の本発明は、公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求を二分木を利用してまとめ、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明プログラムであって、前記利用者装置から前記要求を受信する受信ステップと、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求の値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、前記所定の時間を決定する時刻情報を提供する時刻情報提供ステップと、前記時刻情報提供ステップにおいて提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を前記要求の補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、を前記時刻証明装置に実行させることを要旨とする。

【0050】

請求項38記載の本発明は、請求項37記載の発明において、前記時刻証明書作成ステップは、前記まとめが終了したときに前記時刻情報提供ステップから提供された現ラウンド終了時刻を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成することを要旨とする。

【0051】

請求項39記載の本発明は、請求項38記載の発明において、前記時刻証明要求まとめステップは、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、前記時刻証明書作成ステップは、前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供ステップから提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、前記補完情報取得ステップは、前記直前のルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記送信ステップは、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを要旨とする。

【0052】

請求項40記載の本発明は、公開鍵基盤のもと、所定のデジタル情報に時刻情報の付与を要求する利用者装置とコンピュータネットワークを介して接続されている時刻証明装置が、所定の時間内における複数の前記要求に時刻情報を付すとともに、二分木を利用してまとめ、まとめた値に対してデジタル署名を生成する時刻証明プログラムであって、前記利用者装置から前記要求を受信する受信ステップと、前記要求を受信した時刻情報を提供する時刻情報提供ステップと、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供ステップで提供される前記時刻情報を接続した接続値のダ

イジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する送信ステップと、を前記時刻証明装置に実行させることを要旨とする。

【0053】

請求項4 1記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明装置の時刻証明プログラムであって、前記要求に含まれる時刻証明対象データと、時刻証明要求受付装置が前記要求を受信した時刻である前記第1の時刻情報との組み合わせである前記第2の要求を前記時刻証明要求受付装置から受信する受信ステップと、前記第2の要求を受信した時刻である第2の時刻情報を提供する時刻情報提供ステップと、前記第1の時刻情報と、前記第2の時刻情報の差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめステップと、前記ルート値から部分署名を生成する部分署名生成ステップと、前記部分署名から全体署名を生成し、該全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書、並びに前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値である補完情報を前記利用者装置に送信する前記時刻証明要求受付装置に、前記部分署名を送信する送信ステップと、を前記時刻証明装置に実行させることを要旨とする。

【0054】

請求項4 2記載の本発明は、請求項3 7乃至3 9のいずれか1項に記載の発明において、前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを要旨とする。

【0055】

請求項4 3記載の本発明は、請求項3 7乃至4 2のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを要旨とする。

【0056】

請求項4 4記載の本発明は、請求項3 7乃至4 2のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを要旨とする。

【0057】

請求項4 5記載の本発明は、請求項3 7乃至4 2のいずれか1項に記載の発明において、前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを要旨とする。

【0058】

請求項46記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまとめた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付プログラムであって、前記利用者装置から前記要求を受信する受信ステップと、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てる値を計算する時刻証明要求まとめステップと、前記二分木のルート値を前記時刻証明装置に送信する送信ステップと、前記二分木のルート値に時刻情報を付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記時刻情報を含む時刻証明書を前記時刻証明装置から受信する時刻証明書受信ステップと、前記要求に含まれる時刻証明対象データが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、を前記時刻証明要求受付装置に実行させることを要旨とする。

【0059】

請求項47記載の本発明は、請求項46記載の発明において、前記時刻証明書受信ステップは、前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信することを要旨とする。

【0060】

請求項48記載の本発明は、請求項47記載の発明において、前記時刻証明要求まとめステップは、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、前記送信ステップは、前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直前ルート値及び前記前ラウンド終了時刻を前記前時刻証明装置に送信し、前記時刻証明書受信ステップは、前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、前記補完情報取得ステップは、前記直前ルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記時刻証明書送信ステップは、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信することを要旨とする。

【0061】

請求項49記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記時刻証明要求受付装置の時刻証明要求受付プログラムであって、前記利

用者装置から前記要求を受信する受信ステップと、前記要求に含まれる時刻証明対象データと、前記要求を受信した時刻である前記第1の時刻情報と、の組み合わせである前記第2の要求を前記複数の時刻証明装置それぞれに送信する送信ステップと、前記複数の時刻証明装置それぞれが、前記第1の時刻情報と前記第2の要求を受信した時刻である第2の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信ステップと、前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト、および前記第1の時刻情報を含む時刻証明書を作成する時刻証明書作成ステップと、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得ステップと、前記時刻証明書および前記補完情報を前記利用者装置に送信する時刻証明書送信ステップと、を前記時刻証明要求受付装置に実行させることを要旨とする。

【0062】

請求項50記載の本発明は、請求項46及び48のいずれか1項に記載の発明において、前記二分木のリーフに割り当てられる値は、前記要求に含まれる時刻証明対象データのキー付きハッシュ値であることを要旨とする。

【0063】

請求項51記載の本発明は、請求項49記載の発明において、前記部分署名は、閾値型の分散署名方式であり、前記時刻証明書作成ステップは、前記複数の時刻証明装置から受信した部分署名が所定の数以上ある場合には、全体署名を生成することを要旨とする。

【0064】

請求項52記載の本発明は、請求項46乃至51のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さの違いを1以内に押さえ、ダミーノードを作成しない方法により、動的に構成されることを要旨とする。

【0065】

請求項53記載の本発明は、請求項46乃至51のいずれか1項に記載の発明において、前記二分木は、前記要求の数が確定した後に、深さを単一にして、ダミーノードを作成する方法により、動的に構成されることを要旨とする。

【0066】

請求項54記載の本発明は、請求項46乃至51のいずれか1項に記載の発明において、前記二分木は、深さを単一にして、ダミーノードを作成する方法により、前記要求を受け付ける都度、そこから計算できる二分木の部分を構成していくことを要旨とする。

【0067】

請求項55記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめて、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求に含まれる時刻証明対象データの値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、前記所定の時間を決定する時刻情報を提供する時刻情報提供手段と、前記時刻情報提供手段から提供された前記時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された時刻情報を含む前記時刻証明書を作成する時刻証明書作成手段と、前記要求に含まれる時刻証明対象デー

タが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する前記時刻証明装置から前記時刻証明書および前記補完情報を受信する受信ステップと、前記時刻証明装置に送信した前記要求および前記補完情報から計算した前記二分木のルート値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第1の検証ステップと、前記時刻証明書に含まれる前記デジタル署名が前記ルート値および前記時刻情報を接続した接続値に対して為されたものであるか否かを検証する第2の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0068】

請求項56記載の本発明は、請求項55記載の発明において、前記時刻証明書作成手段は、前記まとめが終了したときに前記時刻情報提供手段から提供された現ラウンド終了時刻を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、前記第2の検証ステップは、前記時刻証明書に含まれる前記デジタル署名が前記ルート値および現ラウンド終了時刻を接続した接続値に対して為されたものであるか否かを検証することを要旨とする。

【0069】

請求項57記載の本発明は、請求項56記載の発明において、前記時刻証明要求まとめ手段は、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割当て、前記時刻証明書作成手段は、前記要求が割り当てられた単位時間の直前の単位時間の終了時に前記時刻情報提供ステップから提供された前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を作成し、前記補完情報取得手段は、前記直前のルート値を割当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記送信手段は、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置に送信し、前記直前ルート値および前記直前ルート値の補完情報から計算した前記二分木のルート値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第3の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0070】

請求項58記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求を二分木を利用してまとめる時刻証明要求受付装置と、前記時刻証明要求受付装置でまとめた値を前記コンピュータネットワークを介して受け付けて、前記まとめた値に時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、前記所定の時間内に受信した前記要求を前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記要求の値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、前記所定の時間を決定する時刻情報を前記ルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された時刻情報を含む前記時刻証明書を前記時刻証明装置から受信する受信手段と、前記要求が割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する前記時刻証明要求受付装置から前記時刻証明書および前記補完情報を受信する受信ステップと、前記時刻証明要求受付装置に送信した前記要求および前記補完情報

から計算した前記二分木のルート値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第1の検証ステップと、前記時刻証明書に含まれる前記デジタル署名が前記ルート値および前記時刻情報を接続した接続値に対して為されたものであるか否かを検証する第2の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0071】

請求項59記載の本発明は、請求項58記載の発明において、前記時刻証明書受信手段は、前記まとめが終了したときに提供された現ラウンド終了時刻を前記二分木のルート値に付して施したデジタル署名、前記ルート値、および前記ルート値に付された前記現ラウンド終了時刻を含み、前記要求の受け付け時刻が、前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、前記第2の検証ステップは、前記時刻証明書に含まれる前記デジタル署名が前記ルート値および前記現ラウンド終了時刻を接続した接続値に対して為されたものであるか否かを検証することを要旨とする。

【0072】

請求項60記載の本発明は、請求項59記載の発明において、前記時刻証明要求まとめ手段は、前記要求が割り当てられた所定の時間を単位時間とし、前記要求が割り当てられた所定の時間の直前の単位時間の終了後計算された直前の単位時間におけるルート値を直前ルート値とすると、前記要求が割り当てられた単位時間に構成される前記二分木の所定のリーフに前記直前ルート値を割り当て、前記時刻証明要求受付装置は、前記直前ルート値に対して前記時刻証明装置により付与された時刻を前ラウンド終了時刻と定義すると、前記直前ルート値及び前記前ラウンド終了時刻を前記前記時刻証明装置に送信する手段を有し、前記時刻証明書受信手段は、前記前ラウンド終了時刻を含み、前記デジタル署名は、前記現ラウンド終了時刻及び前記前ラウンド終了時刻を前記ルート値に付して施したデジタル署名であり、前記要求の受け付け時刻が、前記前ラウンド終了時刻より後でかつ前記現ラウンド終了時刻より前であることを証明する時刻証明書を前記時刻証明装置から受信し、前記補完情報取得手段は、前記直前ルート値を割り当てられた前記二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を直前ルート値の補完情報として取得し、前記受信ステップは、前記直前ルート値及び前記直前ルート値の補完情報を前記利用者装置から受信し、前記直前ルート値および前記直前ルート値の補完情報から計算した前記二分木のルート値と、前記時刻証明書に含まれる前記ルート値と、が一致するか否かを検証する第3の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0073】

請求項61記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、所定の時間内における複数の前記要求に時刻情報を付すとともに、二分木を利用してまとめて、まとめた値に対して時刻情報を付し、デジタル署名を生成する時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、前記要求を受信した時刻情報を提供する時刻情報提供手段と、前記所定の時間内に受信した前記要求に含まれる時刻証明対象データに前記時刻情報提供手段から提供される前記時刻情報を接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた前記ダイジェストの値から前記二分木のルートに割り当てるルート値を計算する時刻証明要求まとめ手段と、前記ルート値に施されたデジタル署名、前記リーフに割り当てられた前記ダイジェスト、および前記要求を受信した時刻情報を含む前記時刻証明書を作成する時刻証明書作成手段と、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する時刻証明装置から前記時刻証明書および前記補完情報を受信する受信ステップと、前記時刻証明装置に送信した前記要求に含まれる時刻証明対象データと前記時刻証明書

に含まれる前記時刻情報とを接続した接続値のダイジェストと、前記時刻証明書に含まれる前記リーフに割り当てられた前記ダイジェストと、が一致するか否かを検証する第1の検証ステップと、前記時刻証明書に含まれるデジタル署名が前記時刻証明書に含まれる、前記リーフに割り当てられた前記ダイジェストおよび前記補完情報から計算された前記二分木のルート値に対して為されたものであるか否かを検証する第2の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0074】

請求項6 2記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置とコンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与する時刻証明要求受付装置と、前記時刻証明要求受付装置と前記コンピュータネットワークを介して接続されており、前記要求に含まれる時刻証明対象データに第1の時刻情報を付与した第2の要求を受け付けて、所定の時間内における、複数の前記第2の要求を二分木を利用してまとめ、まとめた値に部分署名をする複数の時刻証明装置と、を備える公開鍵基盤に基づくタイムスタンプシステムにおける前記利用者装置の時刻証明検証プログラムであって、前記要求に含まれる時刻証明対象データと、前記時刻証明要求受付装置が前記要求を受信した時刻情報である前記第1の時刻情報と、の組み合わせである前記第2の要求を前記複数の時刻証明装置それぞれに送信する送信手段と、前記複数の時刻証明装置それぞれが、前記第1の時刻情報と前記第2の要求を受信した時刻である第2の時刻情報との差が所定の限度内である場合には、前記所定の時間内に受信した前記第2の要求に含まれる前記要求要求内の時刻証明対象データと前記第1の時刻情報とを接続した接続値のダイジェストを前記二分木のリーフに順次割り当てて、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記リーフに割り当てた値から前記二分木のルートに割り当てるルート値を計算し、該ルート値に施した部分署名を、前記複数の時刻証明装置それぞれから受信する部分署名受信手段と、前記部分署名から生成される全体署名、前記リーフに割り当てられた前記ダイジェスト、前記第1の時刻情報を含む時刻証明書を作成する時刻証明書作成手段と、前記ダイジェストが割り当てられた前記リーフから前記二分木のルート値を計算するのに必要な他のノードの値を補完情報として取得する補完情報取得手段と、を有する前記時刻証明要求受付装置から前記時刻証明書および前記補完情報を受信する受信ステップと、前記時刻証明要求受付装置に送信した前記要求要求内の時刻証明対象データと前記時刻証明書に含まれる前記時刻情報とを接続した接続値のダイジェストと、前記時刻証明書に含まれる前記リーフに割り当てられた前記ダイジェストと、が一致するか否かを検証する第1の検証ステップと、前記時刻証明書に含まれる前記全体署名が前記時刻証明書に含まれる、前記リーフに割り当てられた前記ダイジェストおよび前記補完情報から計算された前記二分木のルート値に対して為されたか否かを検証する第2の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0075】

請求項6 3記載の本発明は、請求項3 7乃至6 2のいずれか1項に記載されたプログラムを記録したプログラム記録媒体であることを要旨とする。

【発明の効果】

【0076】

本発明によれば、公開鍵基盤に基づくタイムスタンプシステムにおいて、時刻証明要求を二分木を利用してまとめ、そのまとめたルート値にデジタル署名を施すので、利用者装置から一時的に多くの時刻証明要求があっても、正確な時刻を付した時刻証明をすることができる。

【0077】

また、時刻証明書の有効期限延長を容易に実現することができ、タイムスタンプ・サービスのクライアントは時刻証明書を受領したときに遅滞なく即時に当該時刻証明書の正当性を検証できる。また発行された時刻証明書に付された1つまたは2つの時刻は、その

元となった時刻証明要求がTSAに受け付けられた時刻そのものであるか、或いは受け付けられた時刻の後のある時刻であるか、或いは受け付けられた時刻の前および後の2つの時刻であり、時刻証明書に付された時刻と、時刻証明の受け付けられた時刻の関係を明確にすることができる。

【0078】

さらに、TSAにおけるプログラムによる処理においては、プログラム上のエラーが逸早く検出可能でエラーの影響が限定されるという意味でプログラム上のエラーに対して高い耐性を持つことができ、TSAのサービスが災害やビジネス上の理由で継続不能となったとき、時刻証明書の正当性を保証する方法があり、この保証方法を実行する上で、TSAのサービスのクライアントに対する負荷を小さくすることができる。

【発明を実施するための最良の形態】

【0079】

以下、本発明の実施の形態を図面を用いて説明する。

【0080】

<第1の実施の形態>

図1は、本発明の第1の実施の形態に係るタイムスタンプシステム100のシステム構成図である。同図に示すタイムスタンプシステム100は、TSA10に設けられた時刻証明装置1、TA20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2、利用者30が利用する複数のクライアント装置3i (iは自然数)、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置1がクライアント装置3iからのタイムスタンプ要求(時刻証明要求)に応じて、タイムスタンプ(時刻証明書)をクライアント装置3iに返信するようになっている。

【0081】

時刻証明装置1は、コンピュータネットワーク4を介して時刻情報提供装置2およびクライアント装置3iとデータを送受信する送受信部11、複数のクライアント装置3iからの時刻証明要求に含まれるデータとして送信されたメッセージダイジェスト(メッセージから作成されるハッシュ値)を二分木を用いてまとめる時刻証明要求まとめ部12、時刻証明書を作成する際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部12でまとめられたメッセージダイジェストに対して時刻情報取得部12で取得した時刻情報を付して時刻証明書を作成する時刻証明作成部14、および時刻証明作成部14で作成された時刻証明書を記憶する時刻証明書記憶部15を具備している。

【0082】

ここで、時刻証明要求まとめ部12の二分木を用いて時刻証明要求をまとめる機能について、説明する。図2は、本実施の形態の二分木の一例を示す図である。同図に示す二分木は、予め定められた一定時間(例えば、1秒、このインターバルをラウンドという。)に1つ用意されるものであり、二分木のリーフ(レベル0)には、ラウンド内に複数のクライアント装置3iから受け付けた時刻証明要求に含まれるメッセージダイジェストを順次左側から割り当てようになっている。尚、二分木の構成(高さ(レベルで表現する)、幅(番号で表現する))は、クライアント装置3iからの時刻証明要求の数に応じて変化するものであるため、本実施の形態における二分木は動的に構成されるものであるが、以下においては、図2に示すように、16のリーフを有する二分木の場合について説明し、動的な二分木の構成に関しては、すべての実施の形態に共通の機能であるため、後述することとする。

【0083】

二分木の各ノード(リーフを除く)に割り当てられる値は以下のように計算される。二分木の親における割当値は、左側の子の割当値H'と右側の子の割当値H''を連結(ビット列とビット列の結合)して、その結果のハッシュ値を計算することにより計算されるものであり、これを $h(H' \parallel H'')$ と表す。このようにして下位のレベルの割当値から上

位のレベルの割当値を計算して、最終的に最上位のレベル（ルート）の割当値（ルートハッシュ値） H を求めると、該ルートハッシュ値 H が、時刻証明作成部14においてデジタル署名の対象となるデータである。ここで、レベル j 、番号 i に割り当てられた値を $h(j, i)$ と表して、図2に示す具体例を用いて、ルートハッシュ値 H の算出方法を説明する。

【0084】

あるクライアント装置3*i*から送信された時刻証明要求に含まれるメッセージダイジェストが $h(0, 5)$ であるとき、ルートハッシュ値 H は、 $h(0, 5)$ に $h(0, 4)$ を左から接続しその結果にハッシュ関数 h を適用して、ハッシュ値 h_1 を計算し、該ハッシュ値 h_1 に $h(1, 3)$ を右側から接続しその結果にハッシュ関数 h を適用してハッシュ値 h_2 を計算し、該ハッシュ値 h_2 に $h(2, 0)$ を左側から接続しその結果にハッシュ関数 h を適用してハッシュ値 h_3 を計算し、さらに該ハッシュ値 h_3 に $h(3, 1)$ を右側から接続しその結果にハッシュ関数 h を適用してハッシュ値 $h_4 (= H)$ を計算することにより、求めることができる。即ち、

$H = h(h(h(h(2, 0) \parallel h(h(h(0, 4) \parallel h(0, 5)) \parallel h(1, 3)))) \parallel h(3, 1))$ である。ここで、例えば、 $h(0, 4)$ を左（右）側から接続する場合を（左（右）、 $h(0, 4)$ ）のように表し、 $h(0, 5)$ の値から二分木のルートハッシュ値 H を計算するのに、必要なデータの集合を接続する方向、および接続する順序も含めて表すと、（（左、 $h(0, 4)$ ）、（右、 $h(1, 3)$ ）、（左、 $h(2, 0)$ ）、（右、 $h(3, 1)$ ））となるが、以後、このデータの集合を、二分木における $h(0, 4)$ の補完データとよぶ。尚、補完データは、二分木のリーフに割り当てられる時刻証明要求ごとに作成されるもので、 HK_i （ i は自然数）と表す。

【0085】

また、時刻証明作成部14は、このようにして二分木のルートハッシュ値 H が時刻証明要求まとめ部12において作成されると、このルートハッシュ値 H にそれぞれのラウンドのまとめ処理が終了したときの時刻である現ラウンド終了時刻（例えば、1秒間隔で付される） t を付して署名鍵（秘密鍵） SK を用いてデジタル署名を生成し、該デジタル署名 $sig(SK, H \parallel t)$ 、二分木のルートハッシュ値 H 、時刻 t を含む時刻証明書 $TST(H, t)$ を作成するようになっている。従って、同一ラウンド内において作成される時刻証明書 $TST(H, t)$ は、同一ラウンド内に受け付けた複数の時刻証明要求全てに対して、同一のものとなり、当該のラウンドにおいて受け付けられた全ての時刻証明要求の受け付け時刻より後である時刻 t を含むものとなっている。

【0086】

クライアント装置3*i*は、コンピュータネットワーク4を介して時刻証明装置1とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置1からの時刻証明要求に対する時刻証明書 $TST(H, t)$ を記憶する時刻証明書記憶部34、および時刻証明書 $TST(H, t)$ を検証する時刻証明検証部35を具備している。

【0087】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM（Random Access Memory）等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。

【0088】

このうち、時刻証明装置1の時刻証明要求まとめ部12、時刻情報取得部13および時刻証明作成部14、並びにクライアント装置3*i*の時刻証明要求部33および時刻証明検証部35の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、時刻証明装置1の時刻証明書記憶部15、並びにクライアント装置3*i*のメッセージ記憶部32および時刻証明記憶部34は、上記主記憶装置の機能を備えたものである。

【0089】

次に、以上の構成を有するタイムスタンプシステム100における時刻証明方法、および時刻証明検証方法を図3および図4を用いて説明する。ここで、図3は、時刻証明装置1が時刻証明書 TST(H, t) を作成する動作を説明するフローチャートであり、図4は、クライアント装置3iが時刻証明書 TST(H, t) の検証を行う動作を説明するフローチャートである。

【0090】

まず、時刻証明装置1の動作について説明する。クライアント装置3iから時刻証明装置1の送受信部11を介して時刻証明対象のメッセージダイジェストを含む時刻証明要求を受信すると、時刻証明要求まとめ部12は、このメッセージダイジェストを二分木のリーフに割り当てる(ステップS11, S12)。そして、上記動作は、同一ラウンド内において複数のクライアント装置3iから受信した時刻証明要求に対して、順次行われ、一定時間経過後ラウンドが終了すると、時刻証明要求まとめ部12がそれぞれのリーフに割り当てられたメッセージダイジェストから二分木のルートハッシュ値Hを計算する(ステップS13, S14)。

【0091】

次に、時刻証明作成部14が、このルートハッシュ値Hにその証明を行う日時を示す時刻tを接続し、その接続した結果に対して署名鍵 SK を用いてデジタル署名 $\text{sig}(\text{SK}, H \parallel t)$ を生成する(ステップS15)。そして、このデジタル署名 $\text{sig}(\text{SK}, H \parallel t)$ 、時刻t、ルートハッシュ値Hを含む時刻証明書 TST(H, t) を作成し、さらに、受信したそれぞれの時刻証明要求に対応する二分木の補完データHKiを取得する(ステップS16, S17)。

【0092】

最後に、時刻証明作成部14は、送受信部11を介して、時刻証明書TST(H, t) および補完データHKiを複数のクライアント装置3iに送信する(ステップS18)。

【0093】

これにより、時刻証明装置1は、二分木を用いて時刻証明要求をまとめ、このまとめた値に対してデジタル署名を生成して時刻証明書を発行するので、クライアント装置3iから大量の時刻証明要求が短い期間に集中的にあったとしても、正確な時刻を付した時刻証明を行うことができる。

【0094】

次に、クライアント装置3iの動作について説明する。クライアント装置3iが送受信部31を介して、時刻証明書TST(H, t) および補完データHKiを受信すると、時刻証明検証部35は、以下に示すように検証処理を行う(ステップS21)。

【0095】

まず、時刻証明書TST(H, t)に含まれているルートハッシュ値Hが、クライアント装置3iが時刻証明装置1に送信した時刻証明要求に含まれるメッセージダイジェストと補完データHKiとから計算した二分木のルートハッシュ値Hcal に一致するかどうかを検証する(ステップS22, S23)。

【0096】

次に、署名鍵SKに対応する公開鍵 PK を用いて、デジタル署名 $\text{sig}(\text{SK}, H \parallel t)$ が署名対象のデジタルデータ $H \parallel t$ に対して為されたものであることを検証する(ステップS24, S25)。

【0097】

以上の検証において、検証に成功すれば、時刻証明によって示される時刻に時刻証明要求データは存在していたこと、時刻証明が付与された時刻以降、そのデータは改ざんされていないことを証明することができる(ステップS26)。一方、検証に失敗すれば、データもしくはデジタル署名が改ざんされていることを確認することができる(ステップS27)。これにより、時刻証明装置1が発行した時刻証明書TST(H, t) を的確に検証でき、時刻情報やデータの真正性を第三者に対しても証明することが出来るようになる。

【0098】

尚、第1の実施の形態においては、あるラウンドのルート値に割当て時刻として、当該のラウンドのまとめ処理が終了したときの時刻である現ラウンド終了時刻を用いている。この方式により、当該のラウンドで受け付けられた各時刻証明要求の受け付け時刻が現ラウンド終了時刻より前（時間的に過去）であることが証明される。

【0099】

第1の実施の形態の第1の変形方式として、当該のラウンドの直前のラウンドのまとめ処理が終了したときの時刻を前ラウンド終了時刻と定義し、上記実施の形態における現ラウンド終了時刻の代りに、前ラウンド終了時刻と現ラウンド終了時刻の組を用いることにしてもよい。図18にこの場合の時刻証明書の一例を示す。この際、直前のラウンドのルート値（これを直前ルート値と呼ぶ）を、現在のラウンドの二分木の所定のリーフに割当てるようにしてもよい。

【0100】

図19と図20に、直前ルート値を現在のラウンドの二分木の所定のリーフa0に割当てするための2つの方法を示す。

【0101】

第1の方法は、図19に示すように、リーフa0を現在のラウンドのルートの子ノードとして、現在のラウンドの二分木に含める方法である（リーフa0のレベルとクライアント装置3iからの要求が割り当てられるリーフのレベルは異なる）。

【0102】

第2の方法は、図20に示すように、リーフa0を現在のラウンドの二分木のレベル0の一番左のリーフとする方法である（リーフa0のレベルとクライアント装置3iからの要求が割り当てられるリーフのレベルは同じである）。

【0103】

この場合には、補完情報には、直前ルート値、及び現在のラウンドの二分木における補完情報が含まれる（このように情報を加えた結果である補完情報を拡張補完情報と呼ぶ）。図21に拡張補完情報の一例を示す。尚、この拡張補完情報に含まれる直前ルート値とその現在のラウンドの二分木における補完情報から現在のラウンドのルート値が計算できることを検証すること（これを第3の検証と呼ぶ）により、直前のラウンドにおける二分木の構成が終了したのちに、現在のラウンドの二分木の構成が開始されたことを証明することができる。

【0104】

この第1の変形方式により、当該のラウンドで受け付けられた各時刻証明要求の受け付け時刻が現ラウンド終了時刻より前（時間的に過去）であること及び前ラウンド終了時刻より後（時間的に未来）であることが証明される。

【0105】

第1の実施の形態の第2の変形方式として、上記実施の形態における現ラウンド終了時刻の代りに、前ラウンド終了時刻を用いることにしてもよい。この際、直前ルート値を現在のラウンドの二分木の所定のリーフに割当ててもよく、その方法は上記第1の変形方式と同様である。また、第1の変形方式におけると同様に、拡張補完情報を用いることにしてもよい。

【0106】

この第2の変形方式により、当該のラウンドで受け付けられた各時刻証明要求の受け付け時刻が前ラウンド終了時刻より後（時間的に未来）であることが証明される。

【0107】

また、上記実施の形態においては、リーフに割り当てる値を、クライアント装置3iから送信される時刻証明要求に含まれるメッセージダイジェストとしたが、他のクライアント装置3iに自己の送信したメッセージダイジェストを知られないようにするために、送信したメッセージダイジェストに対して適当な乱数をキーとしたキー付きハッシュ値を計算して、この値をリーフに割り当てる値とし、データの守秘性を高めるようにしてもよい。この場合には、時刻証明装置1からクライアント装置3iに送信されるデータに、キー

となる乱数が追加されることになる。

【0108】

本実施の形態では、時刻証明書の発行のために公開鍵基盤とデジタル署名を用いている（具体的には、図3のステップS15では、署名鍵 SK を用いたデジタル署名を生成し、時刻証明書 TST(H, t) はそれを含んだものとなっている）。従って、デジタル署名の有効性の根拠となる公開鍵証明書に有効期限があるため、時刻証明書の有効性をこの公開鍵証明書の有効期限を越えて保持するためには、時刻証明書の有効期限延長のための処理が必要となる。本実施の形態では、ある1つのラウンドに受け付けられた複数の時刻証明要求に対して、同一のデジタル署名を用いて時刻証明書を発行する。従って、1つのラウンドで発行された時刻証明書の有効期限延長のための処理を、誰か一人（TSA、あるいはクライアントの一人、あるいはそれ以外の第三者）が実行すれば、当該のラウンドに時刻証明要求を出した全てのクライアントの受領する時刻証明書の有効期限延長処理が実現されることになる。従って、時刻証明書を受領した各クライアントが、各々、時刻証明書の有効期限延長処理をしなければならない従来手法（非特許文献1に記載のもの等）に比較して、時刻証明書の有効期限延長処理のためのクライアントの負荷および、該延長処理を行う機関の負荷が著しく軽減されることになる。

【0109】

以上、第1の実施の形態のタイムスタンプシステム100によれば、クライアント装置3iから時刻証明要求を受け付けた時刻証明装置1が、二分木を用いて時刻証明要求をまとめ、このまとめた値に対して時刻情報を付したデジタル署名を生成して時刻証明書を発行するので、クライアント装置3iから大量の時刻証明要求が短い期間に集中する場合であっても、正確な時刻情報を付した時刻証明を行うことができる。また、二分木を利用することにより、時刻証明装置1がクライアント装置3iに送信する時刻証明書および補完データのデータ量を少なくすることができるので、通信負荷を軽減することができる。さらに、時刻証明書の延長処理が必要になった場合には、その処理のためのクライアントの負荷および該延長処理を行う機関の負荷を従来手法に比較して著しく軽減することが出来る。

【0110】

<第2の実施の形態>

図5は、本発明の第2の実施の形態に係るタイムスタンプシステム200のシステム構成図である。同図に示すタイムスタンプシステム200は、要求受付装置5、TSA10に設けられた時刻証明装置6、TA20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2、利用者30が利用する複数のクライアント装置3i（iは自然数）、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、要求受付装置5がクライアント装置3iからのタイムスタンプ要求（時刻証明要求）を受け付けて、受け付けたタイムスタンプ要求をまとめて時刻証明装置6に送信し、時刻証明装置6がまとめられたタイムスタンプ要求に応じて、タイムスタンプ（時刻証明書）を生成し、要求受付装置5を介してクライアント装置3iに返信するようになっている。

【0111】

即ち、タイムスタンプシステム200における要求受付装置5および時刻証明装置6は、タイムスタンプシステム100の時刻証明装置1に相当するものであり、時刻証明装置1の時刻証明要求まとめ部12の機能を要求受付装置5に、時刻情報取得部13および時刻証明作成部14の機能を時刻証明装置6に機能分散して、分散配置したものである。または、既存の時刻証明装置6を利用して、要求受付装置5を加えることにより、タイムスタンプシステム100の時刻証明装置1に相当するシステムを実現するものと見ることも出来る。尚、本実施の形態においては、第1の実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【0112】

要求受付装置5は、コンピュータネットワーク4を介してクライアント装置3iおよび

時刻証明装置6とデータを送受信する送受信部51、複数のクライアント装置3iから送信された時刻証明要求に含まれるメッセージダイジェストを二分木を用いてまとめる時刻証明要求まとめ部12を具備している。

【0113】

時刻証明装置6は、コンピュータネットワーク4を介して時刻情報提供装置2、および要求受付装置5とデータを送受信する送受信部61、時刻証明書を作成する際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部12でまとめられたメッセージダイジェストに対して時刻情報取得部12で取得した時刻情報を付して時刻証明書を作成する時刻証明作成部14、および時刻証明作成部14で作成された時刻証明書を記憶する時刻証明書記憶部15を具備している。

【0114】

尚、第1の実施の形態と同様に、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU: Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)を有する電子的な装置から構成されている。

【0115】

また、タイムスタンプシステム200における時刻証明方法、および時刻証明検証方法は、タイムスタンプシステム100と同様であり、その動作は図3および図4に示す通りであるため、フローチャートを用いての説明は省略するが、タイムスタンプシステム200内のクライアント装置3i、要求受付装置5、および時刻証明装置6間の関係を図6を用いて説明する。

【0116】

図6によれば、クライアント装置3iから時刻証明対象のメッセージダイジェストを含む時刻証明要求が送信されると、要求受付装置5は、一定時間(例えば、1秒)に受け付けたメッセージダイジェストをもとに二分木を構成し、該二分木のルートハッシュ値Hを計算し、該ハッシュ値Hをまとめられた時刻証明要求として時刻証明装置6に送信する。次に、時刻証明装置6は、時刻証明要求を受信したとき時刻tを取得して、受信したハッシュ値Hに対する時刻証明書TST(H, t)を作成し、該時刻証明書TST(H, t)を要求受付装置5に送信する。時刻証明書TST(H, t)を受信した要求受付装置5は、クライアント装置3iから受信した時刻証明要求に対応する二分木の補完データHKiを取得して、時刻証明書TST(H, t)および補完データHKiをクライアント装置3iに送信する。

【0117】

尚、上記第2の実施の形態においては、あるラウンドのルート値Hに割当てた時刻として、当該のラウンドのまとめ処理が終了したのち該ラウンドのルート値を含む時刻証明要求を時刻証明装置6に送付し、時刻証明装置6が該時刻証明要求を受信したときの時刻である現ラウンド終了時刻を用いている。この方式により、当該のラウンドで受け付けられた各時刻証明要求の受け付け時刻が現ラウンド終了時刻より前(時間的に過去)であることが証明される。

【0118】

第2の実施の形態の第1の変形方式として、図22に示すように、要求受付装置5'が当該のラウンドの直前のラウンドにおいて時刻証明装置により生成された時刻証明書(これを直前ラウンド時刻証明書という)を記憶する手段(直前ラウンド時刻証明書記憶部52)を持ち、当該のラウンドのルート値Hと直前ラウンド時刻証明書に含まれる時刻証明装置6によって付された時刻t0(これを前ラウンド終了時刻という)を組合わせたデータH||t0(これを前ラウンド終了時刻付きルート値という)を時刻証明対象データとして時刻証明装置6に対する時刻証明要求に含め、時刻証明装置6はこの時刻証明対象データH||t0に対して、要求受信時の時刻t1を付与してデジタル署名sig(SK, H||t0||t1)を付し時刻証明書を生成してもよい。このように生成された時刻証明書をTST(H, t0, t1)と表す。図23にこの場合の時刻証明書の一例を示す。

【0119】

また、第1の実施の形態の第1の変形方式におけると同様に、直前のラウンドのルート値（これを直前ルート値と呼ぶ）を、現在のラウンドの二分木の所定のリーフに割当て、補完情報には、直前ルート値とその現在のラウンドの二分木における補完情報を含めるようにしてもよい（このように情報を加えた結果である補完情報を拡張補完情報と呼ぶ）。また拡張補完情報に含まれる直前ルート値とその現在のラウンドの二分木における補完情報から現在のラウンドのルート値が計算できることを検証すること（これを第3の検証と呼ぶ）により、直前のラウンドにおける二分木の構成が終了したのちに、現在のラウンドの二分木の構成が開始されたことを証明することができる。

【0120】

第1の変形方式により、当該のラウンドで受け付けられた各時刻証明要求の受け付け時刻が現ラウンド終了時刻より前（時間的に過去）であること及び前ラウンド終了時刻より後（時間的に未来）であることが証明される。

【0121】

第2の実施の形態の第2の変形方式として、図24に示すように、時刻証明装置は、署名対象データに対して時刻情報を付し部分署名を生成する複数の部分時刻証明装置16j（jは自然数）からなる分散時刻証明装置としてもよい。この変形方式においては、要求受付装置5は、複数の部分署名から全体署名を生成する全体署名作成部53を具備する必要がある。

【0122】

第2の変形方式においては、複数ある部分時刻証明装置のうちの所定の数のものが一致した時刻を付すときのみ、全体署名が作成できることになり、時刻証明書に付される時刻の信頼性を向上させることが出来る。

【0123】

本実施の形態でも、第1の実施の形態と同様に、時刻証明書の発行のために公開鍵基盤とデジタル署名を用いている（具体的には、図5の時刻証明装置6が時刻証明書TST(H, t)を生成するときデジタル署名を生成し該時刻証明書に含める）。従って、従って、デジタル署名の有効性の根拠となる公開鍵証明書に有効期限があるため、時刻証明書の有効性をこの公開鍵証明書の有効期限を越えて保持するためには、時刻証明書の有効期限延長のための処理が必要となる。本実施の形態においても、第1の実施の形態と同様に、ある1つのラウンドに受け付けられた複数の時刻証明要求に対して、同一のデジタル署名を用いて時刻証明書を発行する。従って、第1の実施の形態におけると同様に、1つのラウンドで発行された時刻証明書の有効期限延長のための処理を、誰か一人（TSA、あるいはクライアントの一人、あるいはそれ以外の第三者）が実行すれば、当該のラウンドに時刻証明要求を出した全てのクライアントの受領する時刻証明書の有効期限延長処理が実現されることになる。従って、時刻証明書を受領した各クライアントが、各々、時刻証明書の有効期限延長処理をしなければならない従来手法（非特許文献1に記載のもの等）に比較して、時刻証明書の有効期限延長処理のためのクライアントの負荷および、該延長処理を行う機関の負荷が著しく軽減されることになる。

【0124】

以上、第2の実施の形態のタイムスタンプシステム200によれば、第1の実施の形態のタイムスタンプシステム100と同様の効果を得ることができるが、これに加えて、サーバ側の機能を要求機能装置5と時刻証明装置6に機能分散しているため、TSA10に設けられた既存の時刻証明装置6をそのまま利用しつつ、要求受付装置5を新たに設けるだけで、簡単にタイムスタンプシステム200を構築することができるという効果がある。さらに、時刻証明書の延長処理が必要になった場合には、その処理のためのクライアントの負荷および該延長処理を行う機関の負荷を従来手法に比較して著しく軽減することが出来る。

【0125】

<第3の実施の形態>

図7は、本発明の第3の実施の形態に係るタイムスタンプシステム300のシステム構

成図である。同図に示すタイムスタンプシステム300は、TSA10に設けられた時刻証明装置7、TA20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2、利用者30が利用する複数のクライアント装置303i(iは自然数)、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置1がクライアント装置3iからのタイムスタンプ要求(時刻証明要求)に応じて、タイムスタンプ(時刻証明書)を返信するようになっている。

【0126】

タイムスタンプシステム300は、タイムスタンプシステム100と同様のシステム構成をとっているが、時刻証明装置7が、信頼できる第三者機関(TTP; Trusted Third Party)として付与する時刻値について信頼されている場合を前提としており、タイムスタンプシステム100と比べて、より精度の高い時刻値を付与することができるようになっている。尚、本実施の形態においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【0127】

時刻証明装置7は、コンピュータネットワーク4を介して時刻情報提供装置2およびクライアント装置303iとデータを送受信する送受信部11、時刻情報提供装置2から時刻証明書に使用される時刻情報を取得する時刻情報取得部13、クライアント装置303iからの時刻証明要求として送信されたメッセージダイジェストに時刻情報取得部12で取得した時刻情報を付与するとともに二分木を用いてまとめる時刻証明要求まとめ部72、時刻証明要求まとめ部72でまとめられたメッセージダイジェストに対して生成したデジタル署名を含む時刻証明書を作成する時刻証明作成部74、および時刻証明作成部74で作成された時刻証明書を記憶する時刻証明書記憶部15を具備している。

【0128】

ここで、時刻証明要求まとめ部72の二分木を用いて時刻証明要求をまとめる機能について説明する。図8は、本実施の形態の二分木の一例を示す図である。同図に示す二分木は、予め定められた一定時間(例えば、1秒、このインターバルをラウンドという。)に1つ用意されるものであり、二分木のリーフ(レベル0)には、ラウンド内に複数のクライアント装置303iから受け付けたメッセージダイジェストにシーケンス番号、時刻を接続した結果のハッシュ値を順次左側から割り当てるようになっている。ここで、上記接続されるシーケンス番号は、受信したメッセージダイジェストに対するシーケンス番号であり、上記接続される時刻は、メッセージダイジェストを受け付けた時刻で、この時刻は時刻情報取得部12から提供されるものである。従って、本実施の形態においては、第1の実施の形態においてラウンドに対して付与される時刻よりも、より詳細な時刻を付与することが可能となっている。尚、二分木の構成(高さ(レベルで表現する)、各高さのノード数)は、クライアント装置303iからの時刻証明要求の数に応じて変化するものであるため、本実施の形態における二分木も動的に構成されるものであるが、以下においては、図8に示すように、16のリーフを有する二分木の場合について説明する。

【0129】

二分木の各ノード(リーフを除く)に割り当てられる値は、第1の実施の形態と同様に、左側の子の割当値H'と右側の子の割当値H''を接続(ビット列とビット列の結合)して、ハッシュ値を計算することにより、親の割当値は求められるものであり、これを $h(H' \parallel H'')$ と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル(ルート)の割当値(ルートハッシュ値)Hを求めると、該ルートハッシュ値Hが、時刻情報証明部74においてデジタル署名の対象となるデータである。以後、第nラウンドにおいてm番目に受け付けたメッセージダイジェストを $y(n, m)$ 、シーケンス番号を $s(n, m)$ 、時刻を $t(n, m)$ 、リーフに割り当てられるハッシュ値を $H(n; m)$ ($=h(y(n, m) \parallel s(n, m) \parallel t(n, m))$) と表し、また第nラウンドにおいて、レベルjの左からi番目(但し一番左を0番とする)のノードの割当値を $h(n; j, i)$ と表して、ルートハッシュ値Hの算出方法を、図8に示す具体例を用いて説明する。

【0130】

あるクライアント装置3 i から送信されたメッセージダイジェストが $y(n, 4)$ であるとき、リーフに割り当てられるハッシュ値 $H(n; 4)$ は、 $H(n; 4) = h(y(n, 4) \parallel s(n, 4) \parallel t(n, 4))$ である。これにより、ルートハッシュ値 $H(n; 4, 0)$ は、 $H(n; 4)$ に $H(n; 5)$ を右から接続しその結果にハッシュ関数 h を適用して、ハッシュ値 $h1$ を計算し、該ハッシュ値 $h1$ に $H(n; 1, 3)$ を右側から接続しその結果にハッシュ関数 h を適用してハッシュ値 $h2$ を計算し、該ハッシュ値 $h2$ に $H(n; 2, 0)$ を左側から接続しその結果にハッシュ関数 h を適用してハッシュ値 $h3$ を計算し、さらに該ハッシュ値 $h3$ に $H(n; 3, 1)$ を右側から接続しその結果にハッシュ関数 h を適用してハッシュ値 $h4 (= H)$ を計算することにより、求めることができる。この場合、 $H(n; 4)$ の二分木における補完データは、
 ((右, $H(n; 5)$), (右, $H(n; 1, 3)$), (左, $H(n; 2, 0)$), (右, $H(n; 3, 1)$))
 となる。

【0131】

また、時刻証明作成部7 4は、このようにして二分木のルートハッシュ値 $H(n; 4, 0)$ が時刻証明要求まとめ部7 2において作成されると、このルートハッシュ値 $H(n; 4, 0)$ に署名鍵 SK を用いてデジタル署名を生成し、デジタル署名 $\text{sig}(SK, H(n; 4, 0))$ 、シーケンス番号 $s(n, m)$ 、時刻 $t(n, m)$ 、およびリーフ割り当てられたハッシュ値 $H(n; m)$ を含む時刻証明書 $TST(H, t(n, m))$ を作成するようになっている。従って、本実施の形態において作成される時刻証明書 $TST(H, t(n, m))$ は、第1の実施の形態の時刻証明書 $TST(H, t)$ と異なり、同一ラウンド内においても時刻証明要求ごとに異なる時刻証明書 $TST(H, t(n, m))$ となっている。

【0132】

クライアント装置3 0 3 i は、コンピュータネットワーク4を介して時刻証明装置7とデータを送受信する送受信部3 1、デジタル文書などのメッセージを記憶しているメッセージ記憶部3 2、メッセージ記憶部3 2に記憶されているメッセージの時刻証明要求を行う時刻証明要求部3 3、時刻証明装置7からの時刻証明要求に対する時刻証明書 $TST(H, t(n, m))$ を記憶する時刻証明書記憶部3 4、および時刻証明書 $TST(H, t(n, m))$ を検証する時刻証明検証部3 6を具備している。

【0133】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置 (CPU: Central Processing Unit)、プログラムやデータを収納する機能を有するRAM (Random Access Memory) 等からなる主記憶装置 (メモリ) を有する電子的な装置から構成されており、時刻証明装置7の時刻証明要求まとめ部7 2および時刻証明作成部7 4、並びにクライアント装置3 0 3 i の時刻証明検証部3 6の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。

【0134】

次に、以上の構成を有するタイムスタンプシステム3 0 0における時刻証明方法、および時刻証明検証方法を図9および図10を用いて説明する。ここで、図9は、時刻証明装置7が時刻証明書 $TST(H, t(n, m))$ を作成する動作を説明するフローチャートであり、図10は、クライアント装置3 0 3 i が時刻証明書 $TST(H, t(n, m))$ の検証を行う動作を説明するフローチャートである。

【0135】

まず、時刻証明装置7の動作について説明する。クライアント装置3 i から時刻証明装置7の送受信部1 1を介して時刻証明対象のメッセージダイジェストを含む時刻証明要求を受信すると、時刻証明要求まとめ部7 2は、このメッセージダイジェスト $y(n, m)$ に、シーケンス番号 $s(n, m)$ および時刻 $t(n, m)$ を接続しその結果にハッシュ関数を適用して作成したハッシュ値 $H(n; m)$ を二分木のリーフに割り当てる (ステップS 3 1, S 3 2, S 3 3)。そして、上記動作は、同一ラウンド内において複数のクライアント装置3 0 3 i から受信した時刻要求に対して、順次行われ、一定時間経過後ラウンドが終了す

ると、時刻証明要求まとめ部72がそれぞれのリーフに割り当てられたハッシュ値 $H(n; m)$ から二分木のルートハッシュ値 H を計算する(ステップS34, S35)。

【0136】

次に、時刻証明作成部74が、このルートハッシュ値 H に対して署名鍵 SK を用いてデジタル署名 $\text{sig}(SK, H)$ を生成する(ステップS36)。そして、このデジタル署名 $\text{sig}(SK, H)$ 、シーケンス番号 $s(n, m)$ 、時刻 $t(n, m)$ 、リーフに割り当てられたハッシュ値 $H(n; m)$ を含む時刻証明書 $TST(H, t(n, m))$ を作成し、さらに、受信したそれぞれの時刻証明要求に対応する二分木の補完データ HK_i を取得する(ステップS37, S38)。

【0137】

最後に、時刻証明作成部74は、送受信部11を介して、時刻証明書 $TST(H, t(n, m))$ 、および該当する二分木の補完データ HK_i をクライアント装置303iに送信する(ステップS39)。

【0138】

これにより、時刻証明装置7は、時刻を付与した時刻証明要求を二分木を用いてまとめ、このまとめた値に対してデジタル署名を生成して時刻証明書を発行するので、クライアント装置303iから大量の時刻証明要求が短い期間に集中的にあったとしても、正確な時刻を付した時刻証明をより精度高く行うことができる。

【0139】

次に、クライアント装置303iの動作について説明する。クライアント装置303iが送受信部31を介して、時刻証明書 $TST(H, t(n, m))$ 、および二分木の補完データ HK_i を受信すると、時刻証明検証部36は、以下に示すように検証処理を行う(ステップS41)。

【0140】

まず、クライアント装置303iが時刻証明装置7に送信したメッセージダイジェスト $y(n, m)$ と、時刻証明書 $TST(H, t(n, m))$ に含まれているシーケンス番号 $s(n, m)$ および時刻 $t(n, m)$ と、からリーフに割り当てられたハッシュ値 $H_{cal}(n; m)$ を計算し、このハッシュ値 $H_{cal}(n; m)$ が、時刻証明書 $TST(H, t(n, m))$ に含まれている、リーフに割り当てられたハッシュ値 $H(n; m)$ と一致するか否かを検証する(ステップS42, S43)。

【0141】

次に、署名鍵 SK に対応する公開鍵 PK を用いてデジタル署名 $\text{sig}(SK, H)$ が、時刻証明書 $TST(H, t(n, m))$ に含まれている、リーフに割り当てられたハッシュ値 $H(n; m)$ と、補完データ HK_i から計算した二分木のルートハッシュ値 H_{cal} に対して為されたものであることを検証する(ステップS45, S46)。

【0142】

以上の検証において、検証に成功すれば、時刻証明によって示される時刻に時刻証明要求データは存在していたこと、時刻証明が付与された時刻以降、そのデータは改ざんされていないことを証明することができる(ステップS47)。一方、検証に失敗すれば、データもしくはデジタル署名が改ざんされていることを確認することができる(ステップS48)。これにより、時刻証明装置7が発行した時刻証明書 $TST(H, t(n, m))$ を的確に検証でき、時刻情報やデータの真正性を第三者に対しても証明することが出来るようになる。

【0143】

本実施の形態でも、第1の実施の形態と同様に、時刻証明書の発行のために公開鍵基盤とデジタル署名を用いている(具体的には、図7の時刻証明装置7が時刻証明書 $TST(H, t(n, m))$ を生成するときデジタル署名を生成し該時刻証明書に含める)。従って、従って、デジタル署名の有効性の根拠となる公開鍵証明書に有効期限があるため、時刻証明書の有効性をこの公開鍵証明書の有効期限を越えて保持するためには、時刻証明書の有効期限延長のための処理が必要となる。本実施の形態においても、第1の実施の形態と同様に、ある1つのラウンドに受け付けられた複数の時刻証明要求に対して、同一のデジタル署名を用いて時刻証明書を発行する。従って、第1の実施の形態における同様に、1つの

ラウンドで発行された時刻証明書の有効期限延長のための処理を、誰か一人（TSA、あるいはクライアントの一人、あるいはそれ以外の第三者）が実行すれば、当該のラウンドに時刻証明要求を出した全てのクライアントの受領する時刻証明書の有効期限延長処理が実現されることになる。従って、時刻証明書を受領した各クライアントが、各々、時刻証明書の有効期限延長処理をしなければならない従来手法（非特許文献1に記載のもの等）に比較して、時刻証明書の有効期限延長処理のためのクライアントの負荷および、該延長処理を行う機関の負荷が著しく軽減されることになる。

【0144】

以上、第3の実施の形態のタイムスタンプシステム300によれば、タイムスタンプシステム100と同様の効果を得ることができるとともに、クライアント装置303iから時刻証明要求を受け付けた時刻証明装置7が、時刻を付与した時刻証明要求を二分木を用いてまとめ、このまとめた値に対してデジタル署名を生成して時刻証明書を発行するので、精度の高い時刻情報を付した時刻証明書を発行することができる。さらに、時刻証明書の延長処理が必要になった場合には、その処理のためのクライアントの負荷および該延長処理を行う機関の負荷を従来手法に比較して著しく軽減することが出来る。

【0145】

＜第4の実施の形態＞

図11は、本発明の第4の実施の形態に係るタイムスタンプシステム400のシステム構成図である。同図に示すタイムスタンプシステム400は、要求受付装置8、複数のTSA10に設けられた時刻証明装置9j（jは自然数）、複数のTA20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2k（kは自然数）、利用者30が利用する複数のクライアント装置303i（iは自然数）、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、要求受付装置8がクライアント装置303iからのタイムスタンプ要求（時刻証明要求）を受け付けて、受け付けたタイムスタンプ要求に時刻情報を付与して、複数の時刻証明装置9jに送信し、時刻証明装置9jが時刻情報を付与されたタイムスタンプ要求をまとめて部分署名を生成し、生成した部分署名を要求受付装置8に送信し、要求受付装置8が受信した部分署名から全体署名を生成し、全体署名を含むタイムスタンプ（時刻証明書）をクライアント装置3iに返信するようになっている。

【0146】

即ち、タイムスタンプシステム400は、分散署名型のタイムスタンプシステムであり、要求受付装置8で時刻を付与し、複数の各時刻証明装置9jが時刻情報提供装置2kから取得した時刻と、要求受付装置8が付与した時刻との差が所定の限度以内であれば、要求受付装置8で付与した時刻を認めて、デジタル署名（部分署名）を生成するようになっているので、タイムスタンプシステム300と同様に、精度の高い時刻証明を行うことができるようになっている。

【0147】

尚、本実施の形態においては、公開鍵暗号方式に基づいた分散署名の中で最も一般的である分散RSA方式を前提に説明するが、本発明はこの方式に限定されるわけではなく、他の方式を用いることは勿論可能である。また、本実施の形態においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【0148】

要求受付装置8は、コンピュータネットワーク4を介してクライアント装置303iおよび複数の時刻証明装置9jとデータを送受信する送受信部81、クライアント装置303iからの時刻証明要求として送信されたメッセージダイジェストに時刻情報を付与する時刻情報付与部82、複数の時刻証明装置9jで生成された部分署名から全体署名を生成し、この全体署名を含む時刻証明書を作成する全体証明作成部83、および全体証明作成部83で作成された時刻証明書を記憶する時刻証明書記憶部15を具備している。

【0149】

時刻情報付与部82は、さらに詳しくは、クライアント装置303iから送信されたメッセージダイジェスト $y(n,m)$ にシーケンス番号 $s(n,m)$ 、メッセージダイジェストを受け付けた時刻 $t(n,m)$ を組み合わせたデータ $(y(n,m), s(n,m), t(n,m))$ を作成するもので、この組み合わせデータが複数の時刻証明装置9jに送信される時刻証明要求データとなる。また、時刻情報付加部82は、時刻証明装置7の時刻証明要求まとめ部72と同一の二分木を構成する機能を有しており、上記組み合わせデータ $(y(n,m), s(n,m), t(n,m))$ のハッシュ値 $h(y(n,m) \parallel s(n,m) \parallel t(n,m))$ を二分木のリーフに割り当てて、ルートハッシュ値 H を計算できるようになっている。

【0150】

また、全体証明作成部83は、分散RSA方式に基づいて、複数の時刻証明装置9jから送信された部分署名 $psig(PSKj, H)$ から全体署名 $sig(SK, H)$ を生成するようになっている。そして、全体署名、シーケンス番号 $s(n,m)$ 、時刻 $t(n,m)$ 、リーフに割り当てられたハッシュ値 $H(n,m)$ を含む時刻証明書、および時刻情報付加部82で構成した二分木における補完データ HK_i をクライアント装置303iに送受信部81を介して送信するようになっている。

【0151】

時刻証明装置9jは、コンピュータネットワーク4を介して時刻情報提供装置2k及び要求受付装置8とデータを送受信する送受信部91、所定の条件のもと、要求受付装置8から送信された時刻情報を付与されたメッセージダイジェストを二分木を用いてまとめる時刻証明要求まとめ部92、時刻情報提供装置2kから時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部92でまとめられたメッセージダイジェストに対して部分署名を生成する部分証明作成部93、および部分証明作成部93で生成された部分署名を記憶する部分署名記憶部94を具備している。

【0152】

ここで、時刻証明要求まとめ部92は、時刻証明装置7の時刻証明要求まとめ部72と同一の二分木を構成する機能を有しており、要求受付装置8で付与された時刻 t と、時刻証明装置9jが時刻情報提供装置2kから取得した時刻 t' との時刻差が所定の限度以内である場合には、受信した組み合わせデータ $(y(n,m), s(n,m), t(n,m))$ のハッシュ値 $h(y(n,m) \parallel s(n,m) \parallel t(n,m))$ を二分木のリーフに割り当てて、ルートハッシュ値 H を計算できるようになっている。即ち、同一の二分木が要求受付装置8と時刻証明装置9jの双方で構成されるようになっている。

【0153】

また、部分証明作成部93は、二分木のルートハッシュ値 H が部分証明要求まとめ部92において作成されると、このルートハッシュ値 H に部分署名鍵 $PSKj$ を用いて部分署名 $psig(PSKj, H)$ を生成し、この部分署名 $psig(PSKj, H)$ を要求受付装置8に送信するようになっている。

【0154】

尚、以上の各装置は、上記実施の形態の各装置と同様に、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU: Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)を有する電子的な装置から構成されている。即ち、要求受付装置8の時刻情報付与部82および全体証明作成部83、ならびに時刻証明装置9jの時刻証明要求部92および部分証明作成部93は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、時刻証明装置9jの部分署名記憶部94は主記憶装置の機能を備えたものである。

【0155】

次に、タイムスタンプシステム400における時刻証明方法を図12を用いて説明する。ここで、図12は、要求受付装置8と時刻証明装置9jにおける時刻証明書TST(H, t)の作成処理を説明するシーケンス図である。

【0156】

まず、要求受付装置8が、クライアント装置303iから送受信部81を介して時刻証明対象のメッセージダイジェスト $y(n,m)$ を含む時刻証明要求を受信すると、時刻情報付与部82は、このメッセージダイジェスト $y(n,m)$ に、シーケンス番号 $s(n,m)$ および時刻 $t(n,m)$ を組み合わせたデータ $(y(n,m), s(n,m), t(n,m))$ を作成し、これを複数の時刻証明装置9jそれぞれに送受信部81を介して送信する(ステップS51, S52, S53)。

【0157】

時刻証明装置9jは、要求受付装置8から送受信部91を介して組み合わせデータ $(y(n,m), s(n,m), t(n,m))$ を受信すると、時刻証明要求まとめ部92は、組み合わせデータ $(y(n,m), s(n,m), t(n,m))$ に含まれている時刻 $t(n,m)$ と時刻情報取得部13が取得した時刻 t' の差が予め定められた所定の限度内であるか否かを確認、所定の限度内である場合には、この組み合わせデータ $(y(n,m), s(n,m), t(n,m))$ のハッシュ値 $h((y(n,m) \| s(n,m) \| t(n,m)))$ を二分木のリーフに割り当てる(ステップS54, S55, S56)。そして、上記動作は、同一ラウンド内において複数のクライアント装置303iから受信した組み合わせデータ $(y(n,m), s(n,m), t(n,m))$ に対して、順次行われ、一定時間経過後ラウンドが終了すると、時刻証明要求まとめ部92がそれぞれのリーフに割り当てられたダイジェスト $h(y(n,m) \| s(n,m) \| t(n,m))$ から二分木のルートハッシュ値 H を計算する(ステップS58)。

【0158】

次に、部分署名生成部93が、このルートハッシュ値 H に部分署名鍵 PSK_j を用いて部分署名 $psig(SK_j, H)$ を生成し、生成した部分署名 $psig(SK_j, H)$ を要求受付装置8に送信する(ステップS59, S60)。

【0159】

要求受付装置8は、複数の時刻証明装置9jから部分署名部分署名 $psig(PSK_j, H)$ を送受信部81を介して受信すると、全体署名生成部83が、部分署名 $psig(PSK_j, H)$ から全体署名 $sig(SK, H)$ を生成し、この全体署名 $sig(SK, H)$ 、シーケンス番号 $s(n,m)$ 、時刻 $t(n,m)$ 、およびリーフに割り当てられたハッシュ値 $H(n,m)$ を含んだ時刻証明書 $TST(H, t)$ を作成する(ステップS61, S62)。また、時刻情報付加部82で構成した二分木の補完データ HK_i を取得して、時刻証明書 TST および補完データ HK_i をクライアント装置303iに送信する(ステップS63, S64)。

【0160】

尚、時刻証明装置9jにおいて、要求受付装置8が時刻証明要求を受け付けた時刻 t と時刻情報取得部13が取得した時刻 t' の差が予め定められた所定の限度内でない場合には、組み合わせデータ $(y(n,m), s(n,m), t(n,m))$ を破棄して、部分署名 $psig(PSK_j, H)$ は生成しない(ステップS65)。

【0161】

これにより、時刻証明装置9jは、自己で取得した時刻と要求受付装置8で付与した時刻が一定の限度内であれば、時刻を付与した時刻証明要求を二分木を用いてまとめ、このまとめた値に対して部分デジタル署名を生成し、要求受付装置8がこの部分署名から全体署名を生成して、時刻証明書を発行するので、クライアント装置303iから大量の時刻証明要求が短い期間に集中的にあったとしても、正確な時刻を付した時刻証明をより精度高く行うことができる。

【0162】

尚、クライアント装置303iにおける時刻証明書 $TST(H, t)$ の検証を行う動作は、第3の実施の形態と同様であるため、これに関する説明は省略する。

【0163】

本実施の形態でも、第1の実施の形態と同様に、時刻証明書の発行のために公開鍵基盤とデジタル署名を用いている(具体的には、図11の全体署名作成部83が部分署名から全体デジタル署名を作成し、それを用いて時刻証明書を作成している)。従って、従って、

デジタル署名の有効性の根拠となる公開鍵証明書に有効期限があるため、時刻証明書の有効性をこの公開鍵証明書の有効期限を越えて保持するためには、時刻証明書の有効期限延長のための処理が必要となる。本実施の形態においても、第1の実施の形態と同様に、ある1つのラウンドに受け付けられた複数の時刻証明要求に対して、同一のデジタル署名を用いて時刻証明書を発行する。従って、第1の実施の形態における同様に、1つのラウンドで発行された時刻証明書の有効期限延長のための処理を、誰か一人（TSA、あるいはクライアントの一人、あるいはそれ以外の第三者）が実行すれば、当該のラウンドに時刻証明要求を出した全てのクライアントの受領する時刻証明書の有効期限延長処理が実現されることになる。従って、時刻証明書を受領した各クライアントが、各々、時刻証明書の有効期限延長処理をしなければならない従来手法（非特許文献1に記載のもの等）に比較して、時刻証明書の有効期限延長処理のためのクライアントの負荷および、該延長処理を行う機関の負荷が著しく軽減されることになる。

【0164】

以上、第4の実施の形態のタイムスタンプシステム400によれば、分散署名型のタイムスタンプシステムにおいても、タイムスタンプシステム300と同様の効果を得ることができる。即ち、クライアント装置303iから時刻証明要求を受け付けた要求受付装置8は、時刻を付与した時刻証明要求を複数の時刻証明装置9jに送信し、時刻証明装置9jは、自己で取得した時刻と要求受付装置8で付与した時刻が一定の限度内であれば、時刻を付与した時刻証明要求を二分木を用いてまとめ、このまとめた値に対して部分署名をし、要求受付装置8がこの部分署名から全体署名を生成して、時刻証明書を発行するので、精度の高い時刻情報を付した時刻証明書を発行することができる。

【0165】

タイムスタンプ・システムにおいては、タイムスタンプを生成する上で正しい時刻情報の使用が保証されることが望ましい。この際、単独のTSAを全面的に信頼することなく正しい時刻情報の使用について保証するため、当該のTSA以外の第三者が時刻の正しさについて確認する機能を持つことが望ましい。本実施の形態においては、時刻証明書に付する時刻値について、複数のTSAが所定の誤差範囲の中で当該の値を正しいと判断したときのみ、当該の時刻値を含む署名対象データに対するデジタル署名を生成することができるようになっている。このため、一つのTSAの使用する時刻について他のTSAが確認をする機能を実現しており、上記の条件、即ち単独のTSAを全面的に信頼することなく正しい時刻情報の使用について保証するため当該のTSA以外の第三者（当実施の形態においては他のTSA）が時刻の正しさについて確認する機能を持つという条件を満たしている。

【0166】

尚、本実施の形態においては、全体署名の生成のためには全ての署名サーバが同一データに対して部分署名を生成することを要求する（非閾値型の）分散RSA方式を前提にして説明したため、複数の時刻証明装置9jのうち1つでも時刻差が所定の限度を超えていると、要求受付装置8は時刻証明をすることができないが、部分署名する時刻証明装置9jのうちの一定数が部分署名を生成することができれば、最終的に全体署名を生成することができる閾値型分散署名方式（例えば閾値型の分散RSA署名方式）を採用すれば、このような場合においても、時刻証明をすることが可能となる。

【0167】

また、本実施の形態においては、要求受付装置8と時刻証明装置9j間の通信量を減少させるために要求受付装置8および時刻証明装置9jの双方において、同じ二分木を構成するようにしたが、時刻証明装置9jだけで二分木を構成し、二分木の補完データHKiを要求受付装置8に送信する方法により時刻証明を行うようにしてもよい。

【0168】

以上、上記実施の形態における各装置の動作は、各装置に格納されたプログラムを実行することにより実現される。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、コンピュータネットワークを介して配信することも可能である。

【0169】

＜動的な二分木（認証木）の構成方法＞

上記実施の形態において用いられた二分木の動的な構成方法について説明するが、その前提としてまず、二分木の構成に必要な基本関数について説明する。

【0170】

高さ k の二分木は、レベル0からレベル k までのノードで構成されるが、レベル j ($j = 0, 1, \dots, k$) のノードの数は、 $2^{(k-j)}$ であるので、レベル j 、番号 i のノードを (j, i) と表すことにすると、 $i = 0, 1, \dots, 2^{(k-j)} - 1$ となる。以下、実数 x に対して、 $\text{ceiling}(x)$ を x 以上の最小の整数、 $\text{floor}(x)$ を x 以下の最大の整数として、説明する。

【0171】

ノード (j, i) (但し、 $j < k$) の親は、 $(j+1, \text{floor}(i/2))$ であるので、

$\text{parent}(j, i) = (j+1, \text{floor}(i/2))$ と定義する。

【0172】

また、ノード (j, i) (但し、 $0 < j$) の左側の子供は $(j-1, 2i)$ 、右側の子供は $(j-1, 2i+1)$ であるので、

$\text{leftChild}(j, i) = (j-1, 2i)$

$\text{rightChild}(j, i) = (j-1, 2i+1)$ と定義する。

【0173】

このとき、高さ k の二分木のノード (j, i) ($0 \leq i < 2^{(k-j)}$) のルートパス rtPath (ノード (j, i) からルートまでのパスを通過するノード (j, i) の集合で表す) は、 $\text{rtPath}(k, j, i) = ((j, r(j)), \dots, (k, r(k)))$ と表せる。

【0174】

但し、 $j' = j, \dots, k$ に対して、 $r(j')$ は次のように定める。 $r(j) = i$ 、 $r(j'+1) = \text{floor}((r(j') + 1)/2)$ ($j' < k$ とし、 $r(j')$ は既に定まっているものとする)。尚、 $(k, r(k))$ は、二分木のルートを表し、常に $r(k) = 0$ となる。

【0175】

また、高さ k の二分木のノード (j, i) ($0 \leq i < 2^{(k-j)}$) の認証パス $\text{authPath}(k, i, j)$ (ノード (j, i) からルート値を計算するのに必要なノード (j, i) の集合。但し、該ノードを接続する方向(左又は右)の情報も含んでいる) は、 $\text{rtPath}(k, j, i)$ を用いて次のように表せる。

【0176】

$\text{authPath}(k, j, i) = ((j, a(j)), \text{LR}(j)), \dots, ((k-1, a(k-1)), \text{LR}(k-1)))$

ここで、 $r(j')$ が偶数の場合、 $a(j') = r(j') + 1$ 、 $r(j')$ が奇数の場合、 $r(j') - 1$ であり、また、 $r(j')$ が偶数の場合、 $\text{LR}(j') = R$ 、 $r(j')$ が奇数の場合、 $\text{LR}(j') = L$ である(但し、 $j' = j, \dots, k-1$)。

【0177】

上述した基本関数の定義のもと、第1の動的な二分木の構成方法について説明する。この二分木の構成方法は、深さの違いを1以内に押さえ、ダミーノードを作成しない方法である。

【0178】

単位時間(1ラウンドの時間であり、例えば、1秒)に受け付けた時刻証明要求の数を n とすると、高さ k は、 $k = \text{ceiling}(\log_2(n))$ である。高さ k の二分木のリーフ数は最大で 2^k であるので、 $d = 2^k - n$ として、レベル0のノードのうち、 $2d$ 個を消去すれば、時刻証明要求の数 n をダミーノードなしでリーフに割り当てることが可能となる。これは、レベル0のリーフが $2d$ 個減ると、レベル1のリーフが新たに d 個できるので、合計で d 個減り、リーフの数は結局、 $2^k - d = n$ となるからである。

【0179】

以下、 $L1W = 2^{(k-1)}$ (レベル1のノードの個数)、 $L1L = 2^{(k-1)} - d$ (子を有するレベル1のノードの個数) の、 $L0L = 2 \cdot (2^{(k-1)} - d)$ (レベル0のノードの個数) とおくと、 n 個の時刻証明要求のうち、初めの $L0L$ 個をレベル0に配置し、残りをレベル1に配置

するとき、 i 番目の時刻証明要求の配置先を表す関数 $\text{place}(i)$ は次式で表すことができる。

【0180】

$$\text{place}(i) = (0, i) \quad (0 \leq i < L0L)$$

$$\text{place}(i) = (1, L1L + i - L0L) \quad (L0L < i \leq n)$$

ここで、 $\text{place}(i) = (j, i)$ は $\text{place}(i)$ がレベル i' と番号 j' のノードであることを示す。

【0181】

図13は、第1の動的な二分木の構成方法の $n = 10$ の場合の具体例を示すものである。この場合においては、図13に示す通り、 $k = \text{ceiling}(\log_2(10)) = 4$ となり、高さは4である。そして、 $d = 24 - 10 = 6$ であるので、 $6 \times 2 = 12$ 個のレベル0のリーフを消去する。この結果、 $L1W = 23 = 8$ 、 $L1L = 8 - 6 = 2$ 、 $L0L = 2 \times 2 = 4$ となる。従って、レベル0のリーフが4個、レベル1のリーフが6個で、リーフの合計数は $n = 10$ となる。この結果、図13に示すような二分木を動的に作成することができる。

【0182】

次に、第2の動的な二分木の構成方法について説明する。この二分木の構成方法は、深さを単一にして、ダミーノードを作成する方法である。

【0183】

単位時間（1ラウンドの時間であり、例えば、1秒）に受け付けた時刻証明要求の数を n とすると、高さ k は、 $k = \text{ceiling}(\log_2(n))$ である。高さ k の二分木のリーフ数は最大で 2^k であるので、0から $n-1$ までの n 個の時刻証明要求をレベル0のノード $(0, 0)$ からノード $(0, n-1)$ に割り当てる。ここで、レベル0に割り当てられた、最も右のノード $(0, n-1)$ に対して、ルートパス $\text{rtPath}(k, 0, n-1)$ を計算し、その結果を $((0, r(0)), \dots, (k, r(k)))$ とする。

【0184】

次に、各レベル j ($j = 0, \dots, k-1$) においては、以下の手順を実行するものとする。

【0185】

$r(j)$ が偶数のとき、ノード $(j, r(j)+1)$ をダミーノードとする。

【0186】

$r(j) + 1 < i < 2(k-j)$ となる各 i に対して、ノード (j, i) は消去される。

【0187】

$r(j)$ が奇数のとき、 $r(j) + 1 \leq i < 2(k-j)$ となる各 i に対して、ノード (j, i) は消去される。また、ルートにあるレベル k については、何も行わない。

【0188】

以上のような方法に基づいて構成される二分木は、ダミーノードは各レベルの右端でのみ現れる、および作成されるダミーノードの数は、 k 以下であるという性質を有する。

【0189】

図14は、第2の動的な二分木の構成方法の $n = 9$ の場合の具体例を示す図である。この場合においては、図14に示す通り、 $k = \text{ceiling}(\log_2(9)) = 4$ となり、高さは4である。そして、9個の時刻証明要求をノード $(0, 0) \dots (0, n-1)$ に割り当てると、レベル0において時刻証明要求が割り当てられた最も右のノードは $(0, 8)$ である。

【0190】

ここで、ノード $(0, 8)$ のルートパス $\text{rtPath}(4, 0, 8)$ は

$\text{rtPath}(4, 0, 8) = ((0, 8), (1, 4), (2, 3), (3, 1), (4, 0))$ となる。これにより、各レベルでの手順は、以下の通りになる。

【0191】

レベル0では、 $(0, 9)$ がダミーノードになり、番号10以降が消去される。レベル1では、 $(1, 5)$ がダミーノードとなり、 $5 < i < 23 = 8$ であれば、ノード (j, i) は削除される。レベル2では、ノード $(2, 3)$ がダミーノードになる。レベル3および4においては、

ダミーノードも消去されるノードもない。この結果、図14に示すような二分木を動的に作成することができる。

【0192】

次に、第3の動的な二分木の構成方法について説明する。第1および第2の動的な二分木の構成方法は、ともに受け付けた時刻証明要求の数が確定した後に、二分木を構成する方法であったが、この方法は、第2の動的な二分木の構成方法をベースに、インクリメンタルに二分木を構成する方法である。ここで、インクリメンタルとは、時刻証明要求を受け付ける都度、そこから計算できる二分木の部分を計算していくという意味である。この意味で、前もって定めた時間間隔（ラウンドの時間）に受け付ける時刻証明要求の数は予想できないものとする。以下では、受け付ける時刻証明要求の数は予想できないが、その上界Nは見積もることができるとして説明する。尚、この方法においては、第2の動的な二分木の構成方法と同様に、時刻証明要求はすべてレベル0に割り付けられるものとする（ダミーノードを使用する方法である）。

【0193】

図15は、第3の動的な二分木の構成方法のアルゴリズムを示すものであり、該アルゴリズムに従って二分木がインクリメンタルに構成されるようになっている。ここで、前提として以下の定義を行う。

【0194】

・ $K = \text{ceiling}(\log_2(N))$ とする。

【0195】

・ n は受け付けた時刻証明要求の数を示す整数変数とする。初期値は0である。

【0196】

・ k は定められた時間間隔が終了したときの二分木の高さを表す変数とする。

【0197】

($K+1$) 個のカウンタの列を、 $i(0), \dots, i(K)$ とする。ここで、 $i(j)$ の初期値は0である ($j=0, \dots, K$)。 $i(j)$ はレベル j において、既に生成されたノードの数を表すと同時に、次にレベル j に作成されるノードの番号を表す。

【0198】

・ ($K+1$) 個のブール変数の列を、 $b(0), \dots, b(K)$ とする。ここで、 $b(j)$ の初期値は false である ($j=0, \dots, K$)。 $b(j)$ は、レベル j にダミーノードがあるか否かを表す。

【0199】

・ ($K+1$) 個の配列の列を、 $A(0), \dots, A(K)$ とする。各配列は、 $2^{(K-j)}$ の長さを持ち、レベル j のノードに割り付けられる値を保持する ($j=0, \dots, K$)。ノード (j, i) に対して、 $A(j, i)$ は、 $A(j)[i]$ を表すものとする。ノード (j, i) の左側の子が (j', i') のとき、 $A(\text{leftChild}(j, i))$ は $A(j')[i']$ を表す。

【0200】

・ r はダミーノードに割り当てるダミー値を保存する変数である。

【0201】

・ $R(j, i)$ は2つの引数 i, j に対してノード (j, i) に割り当てるべきダミー値を計算する関数である。

【0202】

・ $x, x0, x1, x2$ は、ノードに割り当てる値を表す変数である。

【0203】

・ $x1 \parallel x2$ は、バイト列で表された2つの値の接続である。

【0204】

・ $h(x)$ は x のハッシュ値を計算する関数である。

【0205】

このような定義のもと、図15の処理手順1が終了すると（定められた時間が終了すると）、 n は、受け付けた時刻証明要求の数、 k は生成された二分木の高さ、 $i(j)$ は、レベル j のノードの数、 $b(j)$ は、レベル j にダミーノードがあるか否か、 $A(j)$ は、レベル j のノード

に割り付けられた値、をそれぞれ有することになる(但し、 $j = 0, \dots, k$)。

【0206】

図16は、第3の動的な二分木の構成方法の $n = 9$ の場合の具体例を示す図である。即ち、定められた時間間隔が終了したとき、 $n = 9$ であったとする。このとき、 $k = \text{ceil}(\log_2(9)) = 4$ となり、高さは4の二分木を構成することになる。尚、0から $n - 1$ までの n 個の時刻処理要求は、処理手順1により、既にノード $(0, 0), \dots, (0, n-1)$ に割り当てられている。また、処理手順1により、 $i(0) = 9, i(1) = 4, i(2) = 2, i(3) = 1, i(4) = 0$ となっている。

【0207】

このとき、処理手順2の(2.2)から、ノード $(0, 9)$ のノートパス $\text{rtPath}(4, 0, 8)$ は、 $\text{rtPath}(4, 0, 8) = ((0, 8), (1, 4), (2, 2), (3, 1), (4, 0))$ となる。これから、各レベルの手順は、以下の通りになる。

【0208】

レベル0においては、ステップ(2.3.2.1)より、ノード $(0, 9)$ がダミーノードになる。レベル1においては、ステップ(2.3.3.1)より、ノード $(1, 4)$ に値が割り付けられ、 $(1, 5)$ がダミーノードになる。レベル2においては、ステップ(2.3.3.1)より、ノード $(0, 2)$ に値が割り付けられ、 $(0, 3)$ がダミーノードになる。レベル3においては、ステップ(2.3.3.1)により、ノード $(3, 1)$ に値が割り付けられる。レベル4においては、ステップ(2.3.3.1)により、ノード $(4, 0)$ に値が割り付けられる。

【0209】

この結果、図16に示すような二部木をインクリメンタルに構成することができる。

【0210】

尚、上記実施の形態におけるタイムスタンプシステム100、200、300および400は、上述した動的な二分木の構成方法のいずれをも採用できるものであり、これにより、クライアント装置3iおよび303iからの時刻証明要求の量的変化に柔軟に対応することができるので、スケーラビリティの高いタイムスタンプシステムを構築することが可能となる。

【図面の簡単な説明】

【0211】

【図1】本発明の第1の実施の形態に係るタイムスタンプシステムの構成を説明する図である。

【図2】本発明の第1の実施の形態における二分木を説明する図である。

【図3】本発明の第1の実施の形態に係る時刻証明装置が時刻証明書を発行する動作を説明するフローチャートである。

【図4】本発明の第1の実施の形態に係るクライアント装置が時刻証明書の検証を行う動作を説明するフローチャートである。

【図5】本発明の第2の実施の形態に係るタイムスタンプシステムの構成を説明する図である。

【図6】本発明の第2の実施の形態に係るタイムスタンプシステムの動作を説明するシーケンス図である。

【図7】本発明の第3の実施の形態に係るタイムスタンプシステムの構成を説明する図である。

【図8】本発明の第3の実施の形態における二分木を説明する図である。

【図9】本発明の第3の実施の形態に係る時刻証明装置が時刻証明書を発行する動作を説明するフローチャートである。

【図10】本発明の第3の実施の形態に係るクライアント装置が時刻証明書の検証を行う動作を説明するフローチャートである。

【図11】本発明の第4の実施の形態に係るタイムスタンプシステムの構成を説明する図である。

【図12】本発明の第4の実施の形態に係るタイムスタンプシステムの動作を説明するシー

ケンス図である。

【図13】深さの違いを1以内に押さえ、ダミーノードを作成しない動的な二分木の構成方法を説明する図である。

【図14】深さを単一にして、ダミーノードを作成する動的な二分木の構成方法を説明する図である。

【図15】インクリメンタルに二分木を構成する方法のアルゴリズムを説明する図である。

【図16】インクリメンタルに二分木を構成する方法を説明する図である。

【図17】タイムスタンプシステム概念を説明する図である。

【図18】本発明の第1の実施の形態に係るタイムスタンプシステムの変形例における時刻証明書の構成を示す図である。

【図19】本発明の第1の実施の形態の変形例における直前ラウンドのルート値を現ラウンドの二分木のリーフに割り当てる方法1を説明する図である。

【図20】本発明の第1の実施の形態の変形例における直前ラウンドのルート値を現ラウンドの二分木のリーフに割り当てる方法2を説明する図である。

【図21】本発明の第1の実施の形態の変形例における補完情報の構成を示す図である。

【図22】本発明の第2の実施の形態に係るタイムスタンプシステムの変形例1の構成を示す図である。

【図23】本発明の第2の実施の形態に係るタイムスタンプシステムの変形例における時刻証明書の構成を示す図である。

【図24】本発明の第2の実施の形態に係るタイムスタンプシステムの変形例2の構成を示す図である。

【符号の説明】

【0212】

1, 6, 7, 9 時刻証明装置

2 時刻情報提供装置

3, 303 クライアント装置

4 コンピュータネットワーク

5, 5', 5" 要求受付装置

10 TSA

11, 31, 51, 61, 81, 91 送受信部

12, 72, 92 時刻証明要求まとめ部

13 時刻情報取得部

14, 74 時刻証明作成部

15 時刻証明書記憶部

16 部分時刻証明装置

20 TA

30 利用者

32 メッセージ記憶部

33 時刻証明要求部

34 時刻証明書記憶部

35, 36 時刻証明検証部

52 直前ラウンド時刻証明書記憶部

53 全体署名作成部

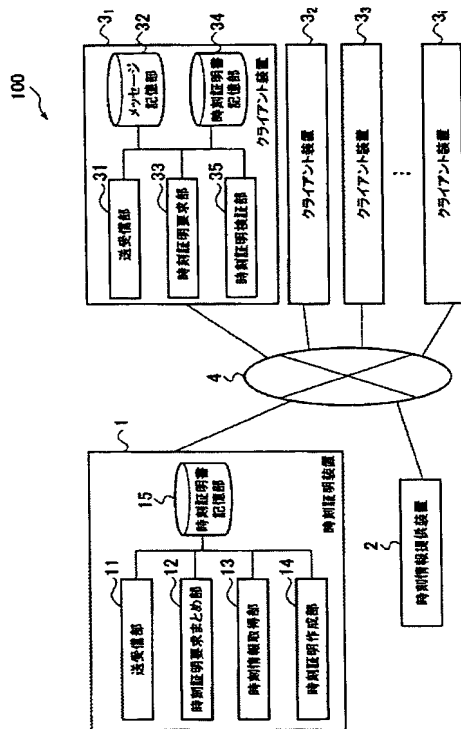
82 時刻情報付加部

83 全体証明作成部

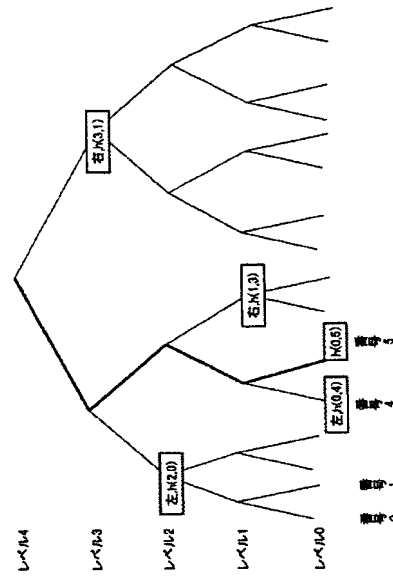
93 部分証明作成部

100, 200, 200', 200", 300, 400, 900 タイムスタンプシステム

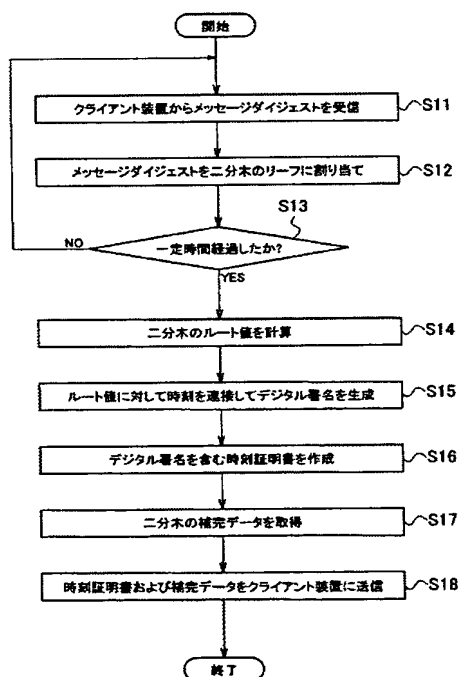
【図1】



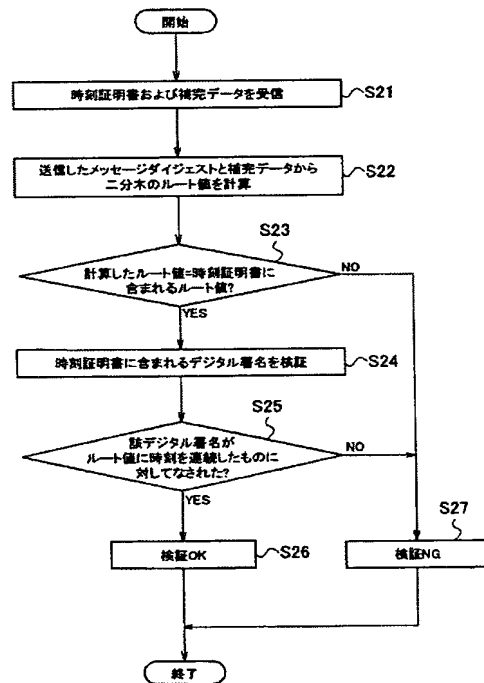
【図2】



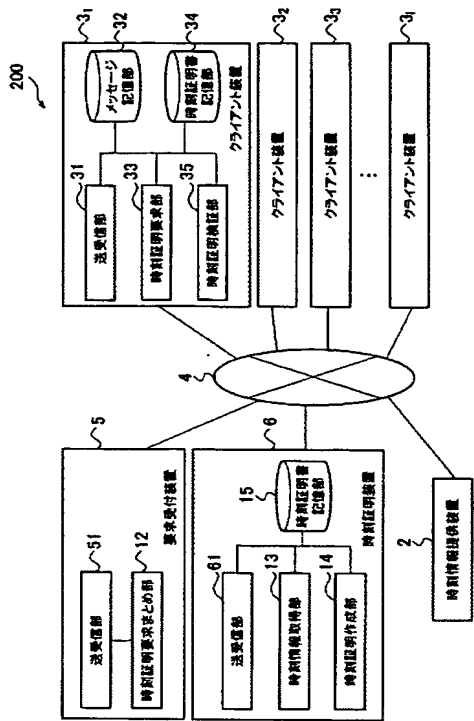
【図3】



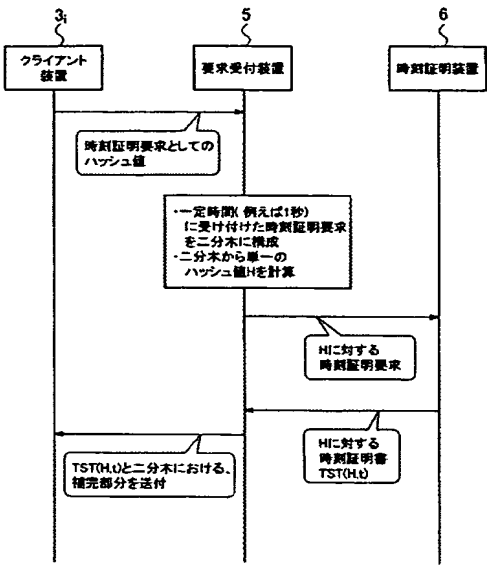
【図4】



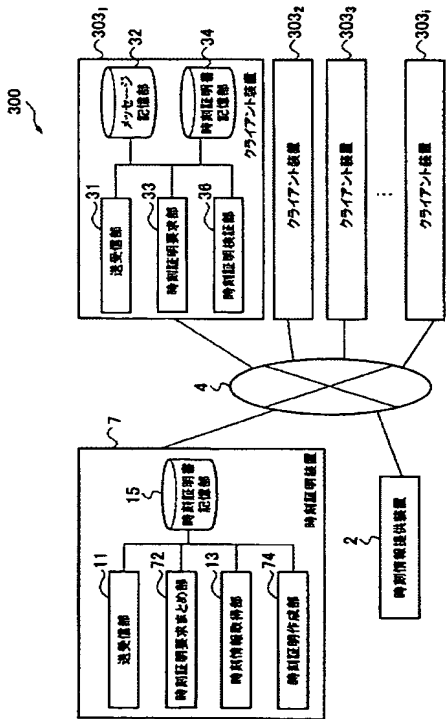
【図5】



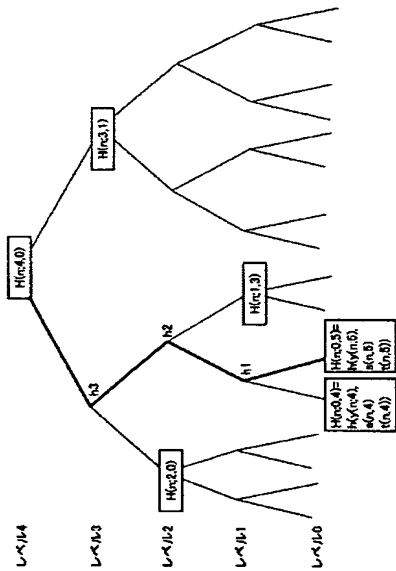
【図6】



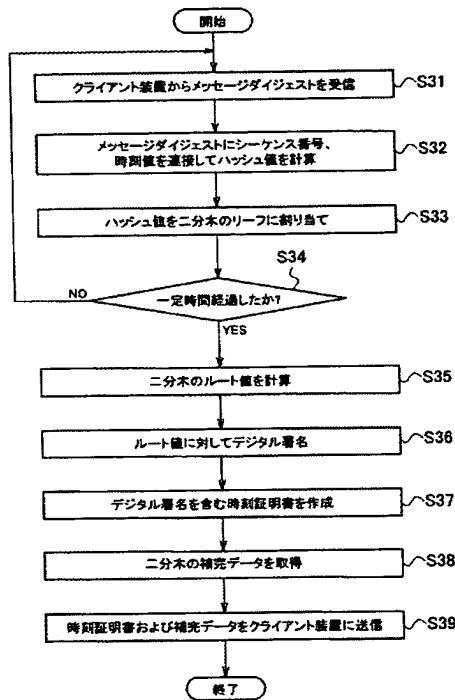
【図7】



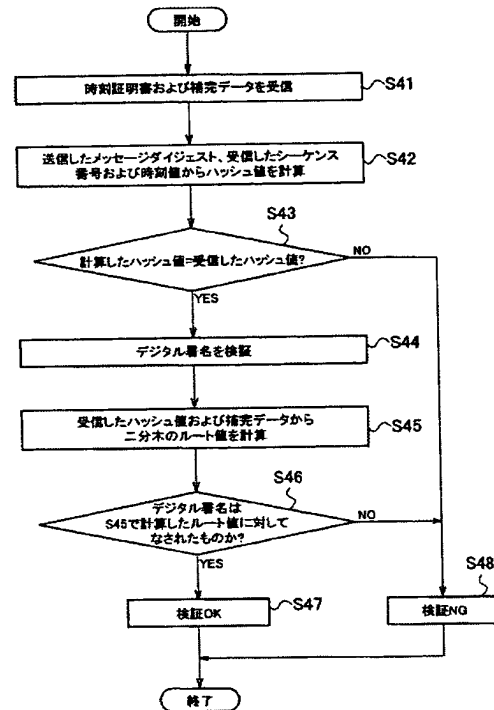
【図8】



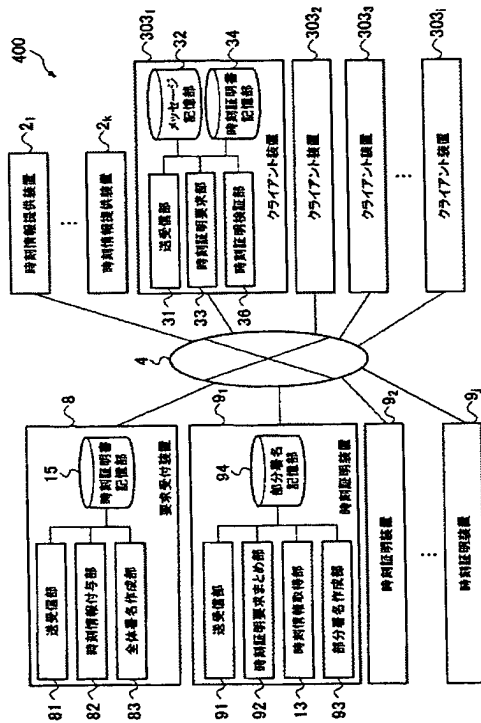
【図9】



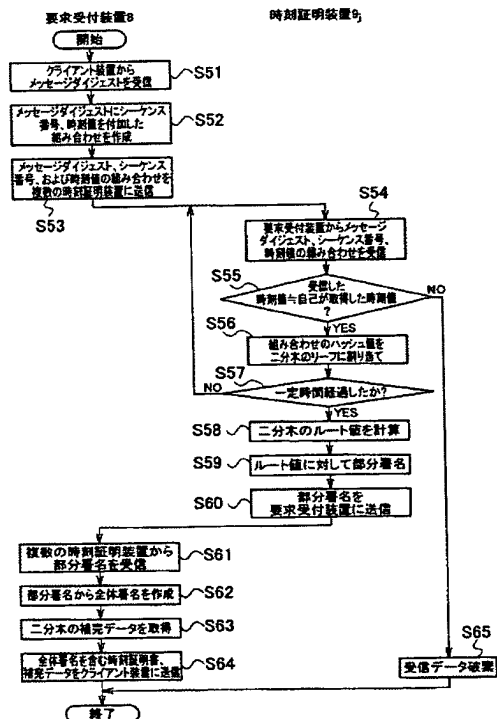
【図10】



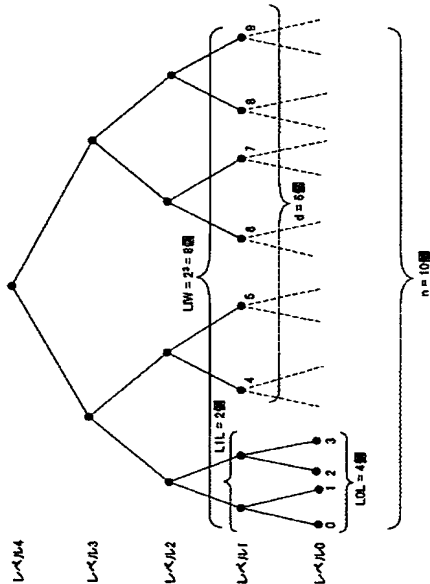
【図11】



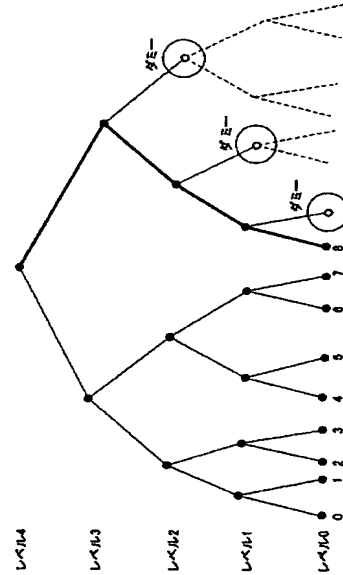
【図12】



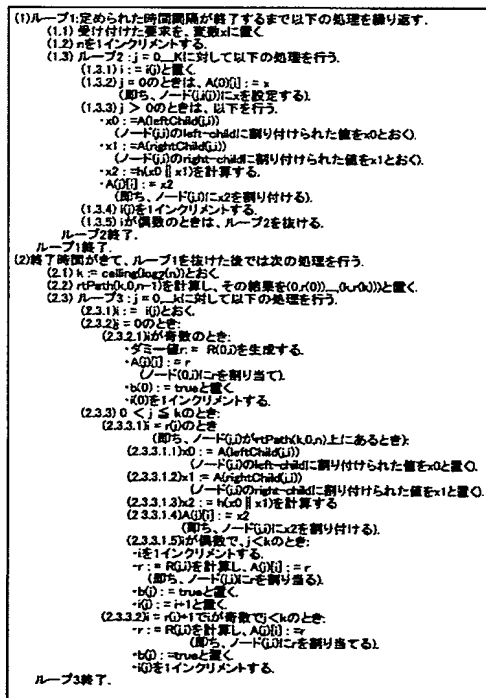
【図13】



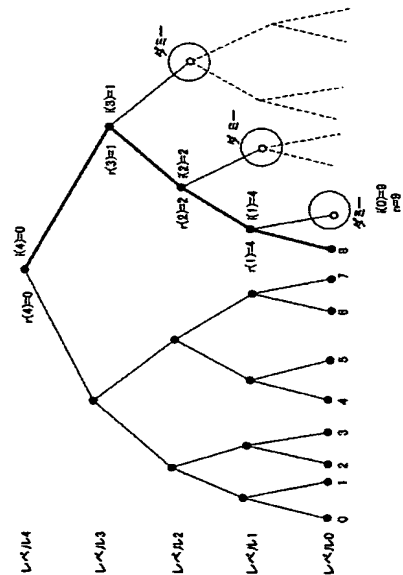
【図14】



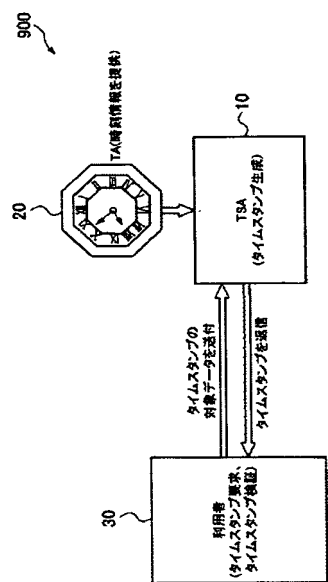
【図15】



【図16】



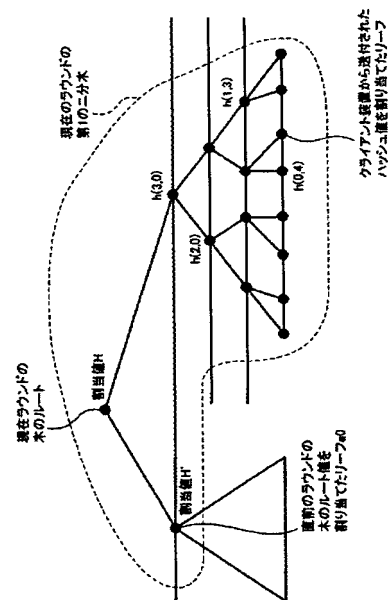
【図17】



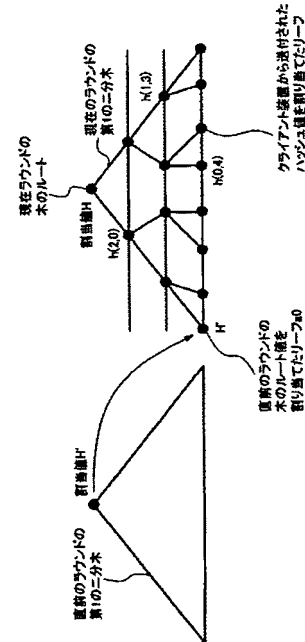
【図18】

| 項目 | 記号 | 値の例 |
|--------------------------|--|-----|
| 時刻証明装置が付与する 現ラウンド終了時刻 | t_1 | |
| 時刻証明装置が付与する 前ラウンド終了時刻 | t_0 | |
| 現在のラウンドの 二分木のルート値 | H | |
| デジタル署名 | $\text{sig}(\text{SK}, H \parallel t_0 \parallel t_1)$ | |

【図19】



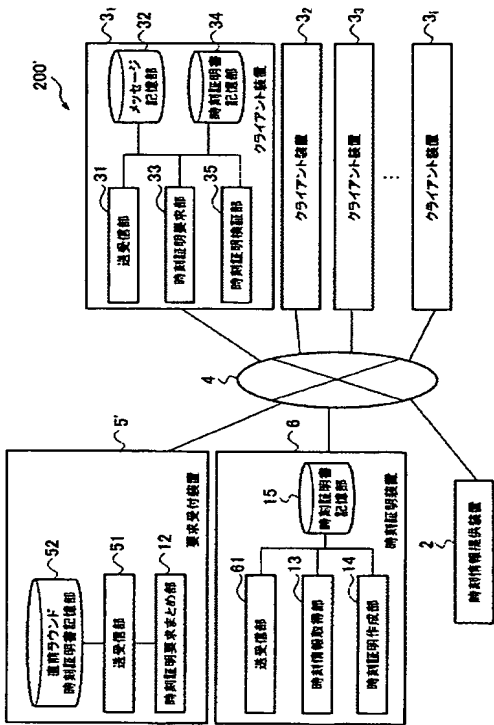
【図20】



【図21】

| 項目 | 記号 | 値の例 |
|------------------------------|------|--|
| 補充情報 | HK1 | $[(L, H(0, 4)), (R, H(1, 3)), (L, H(2, 0)), (L, H)]$ |
| 前のラウンドのルート値 | H' | |
| 前のラウンドのルート値が割当てられたリーフの1次補充情報 | HK1' | $[(R, H(3, 0))]$ |

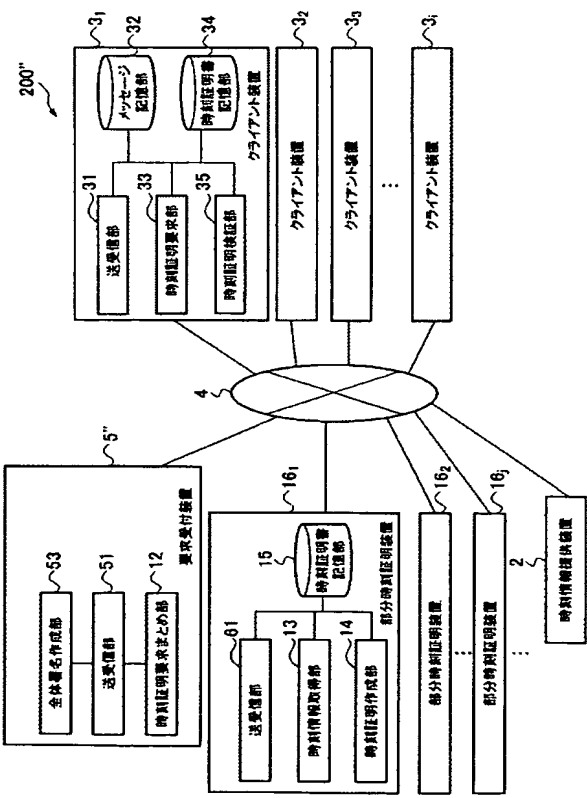
【図22】



【図23】

| 項目 | 記号 | 値の例 |
|------------------------------|--|-----|
| 時刻証明装置が付与する 現ラウンド終了時刻 | t1 | |
| 時刻証明要求受付装置が付与する 前ラウンド終了時刻 | t0 | |
| 現在のラウンドの 二分木のルート値 | H | |
| デジタル署名 | $\text{sig}(\text{SK}, H \parallel t0 \parallel t1)$ | |

【図24】



(6 0)

特開2005-130488 (P2005-130488A)